



KULA
PARTNERS



PROTECTION OF PERSONAL INFORMATION POLICY
KULA PARTNERS (PTY) LTD

FSP 43066



Version	3
Frequency of Review	Annually
Responsible Business Unit	Compliance Department

POLICY STATEMENT

- Any reference to Kula Partners will be interpreted to include the “policy owner”.
- Kula Partners’s governing body, its employees, volunteers, contractors, suppliers and any other person acting on behalf of the organisation are required to familiarise themselves with the policy’s requirements and undertake to comply with the stated processes and procedures.

POLICY ADOPTION

By signing this document, I authorise Kula Partners’s approval and adoption of the processes and procedures outlined herein.

Name	Johannes Swanepoel
Capacity	Key Individual

Table of Contents

POLICY STATEMENT	3
POLICY ADOPTION	3
1. INTRODUCTION	5
2. DEFINITIONS	5
3. OBJECTIVES.....	5
4. COLLECTION OF PERSONAL INFORMATION.....	5
4.8. Collection of employee information	6
4.9. Use of employee information	7
4.10. Collection of member, client and supplier information.....	7
4.11. Disclosure of personal information.....	8
5. SAFEGUARDING OF PERSONAL INFORMATION AND CONSENT	8
6. DIRECT MARKETING	10
7. TRANSFER OF INFORMATION OUTSIDE OF SOUTH AFRICA	10
8. SURVEILLANCE SYSTEMS	10
9. SECURITY BREACHES.....	11
10. ACCESS AND CORRECTION OF PERSONAL INFORMATION	11
11. RETENTION OF RECORDS	12
12. AMENDMENTS TO THIS POLICY	12
13. REQUESTS FOR INFORMATION	12
ANNEXURE.....	13
LEGISLATIVE MAPPING REGISTER.....	13

1. INTRODUCTION

- 1.1. Kula Partners processes personal information of its employees, members, clients and other data subjects from time to time. As such, it is obliged to comply with the Protection of Personal Information Act 4 of 2013 (**POPI**) as well as the Promotion of Access to Information Act 2 of 2000 (**PAIA**).
- 1.2. In line with this, Kula Partners is committed for protecting its member, client, employees and other data subjects' privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.
- 1.3. This Policy sets out the ways in which Kula Partners deals with such personal information and provides clarity on the general purpose for which the information is used, as well as how data subjects can participate in this process in relation to their personal information.

2. DEFINITIONS

- 2.1. **"Biometric Information"** means the physical, physiological or behavioural identification, including finger printing, amongst others.
- 2.2. **"Processing"** means:
 - The collection, receipt, recording organisation, collation, storage, updating, modification, retrieval, alteration, consultation or use.
 - Dissemination by means of transmission, distribution or making available in any form.
 - Merging, linking, erasure or destruction of information.
- 2.3. **"Regulator"** means the Information Regulator established in terms of POPI.

3. OBJECTIVES

The objectives of this policy are to:

- 3.1. Ensure legislative compliance (POPI and PAIA) in respect of all personal information that Kula Partners collects and processes.
- 3.2. Inform employees and clients as to the use of their personal information, its disclosure and destruction.
- 3.3. Ensure that personal information is only used for the purpose for which it was collected.
- 3.4. Prevent unauthorised access and use of personal information.

4. COLLECTION OF PERSONAL INFORMATION

- 4.1. Kula Partners collects and processes various information pertaining to its employees, members, clients and suppliers. The information collection is based on need and it will be processed for that need and purpose only. Whenever possible, Kula Partners will inform the relevant party of the information required and which information is deemed optional.
- 4.2. The employee, member or client will be informed of the consequences of failing to provide such personal information and any prejudice which may be incurred due to non-disclosure. For example, Kula Partners may not be able to employ an individual without certain personal information relating to that individual or the organisation may not be able to

render services to a client in the absence of certain information which is required.

- 4.3. Kula Partners will process information in a manner that is lawful and reasonable (it will not infringe the privacy of the individual or company).
- 4.4. Where consent is required for the processing of information, such consent will be obtained.
- 4.5. Information will be processed under the following circumstances:
 - When carrying out actions for the conclusion or performance of a contract.
 - When complying with an obligation imposed by law.
 - For the protection of a legitimate interest of the data subject.
 - It is necessary to pursue the legitimate interests of Kula Partners or for an authorised third party to whom the information is supplied.
- 4.6. Examples of the personal information Kula Partners collects includes but not limited to:
 - Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, social origin, colour, sexual orientation, age, physical, mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of an employee.
 - Information relating to the education or the medical, financial, criminal or employment history (this includes disciplinary action) of an employee.
 - Banking and accounting information.
 - Contact information.
 - Trade union membership and political persuasion.
 - Any identifying number, symbol, email address, telephone number or location information.
 - online identifier or other assignment to the employee, member or client.
 - The Biometric Information of the employee, member, client or data subject.
 - The personal opinions, views or preferences of an employee (also performance appraisals or correspondence) and the views or opinions of another individual about the person.
- 4.7. Kula Partners will not process special personal information without complying with the specific provisions of the POPI Act. Special information includes personal information concerning:
 - The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sex life or Biometric Information of a data subject.
 - The criminal behaviour of a data subject, where such information relates to the alleged commission by a data subject of any offence committed or the disposal of such proceedings.

4.8. Collection of employee information

- 4.8.1. For the purposes of this policy, employees include potential, past and existing employees

of Kula Partners. Independent contractors are treated on the same basis where the collection of information is concerned.

4.8.2. When appointing new employees or contractors, Kula Partners requires information, including, but not limited to that listed above, from prospective employees or contractors, to process the information on the systems. Such information is reasonably necessary for Kula Partners's record purposes, as well as to ascertain if the prospective employee or contractor meets the requirements, for the position which he is being appointed or contracted and is suitable for appointment.

4.8.3. Kula Partners will use and process such employee information, as set out below for including, but not limited to, its employment records and to make lawful decisions in respect of that employee and its business.

4.9. Use of employee information

Employees personal information will only be used for the purpose for which it was collected and intended. This includes but is not limited to:

- Submissions to the Department of Labour.
- Submission to the Receiver of Revenue.
- For audit and recordkeeping purposes.
- In connection with legal proceedings.
- In connection with and to comply with legal and regulatory requirements.
- In connection with any administrative functions of Kula Partners.
- Disciplinary action or any other action to address the employee's conduct or capacity.
- In respect of any employment benefits that the employee is entitled to.
- Pre- and post-employment checks and screening.
- Any other relevant purpose to which the employee has been notified.
- Should information be processed for any other reason, the employee will be informed accordingly.

4.10. Collection of member, client and supplier information

4.10.1. For the purposes of this Policy, clients include potential, past and existing members and clients. Suppliers include all vendors which contract with Kula Partners whether once-off or recurring, in respect of products and services.

4.10.2. Kula Partners collects and processes its members', clients', and suppliers' personal information, such as that mentioned hereunder. The type of information will depend on the need for which it is collected and will be processed for that purpose only.

4.10.3. Further examples of personal information collected from clients include but is not limited to:

- The member, client or supplier's identity number, name, surname, address, postal code.

- The member, client or supplier's residential and postal address.
- Contact information.
- Banking details.
- Company registration number.
- Full name of the legal entity.
- Tax and VAT number.
- Details of the person responsible for the client's or supplier's account.

4.10.4. Kula Partners also collects and processes member or client's personal information for marketing purposes to ensure that its products and services remain relevant to our clients and potential clients.

4.10.5. Use of member, client or supplier information:

The member, client or supplier's personal information will only be used for the purpose for which it was collected and as agreed. This may include, but not be limited to:

- Providing products or services to members or clients.
- In connection with sending accounts and communication to a member or client in respect of services rendered.
- Payment of suppliers and communication in respect of services rendered.
- Referral to other service providers.
- Confirming, verifying and updating member, client or supplier details.
- Conducting market or customer satisfaction research.
- For audit and record keeping purposes.
- In connection with legal proceedings.
- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

4.11. Disclosure of personal information

4.11.1 Kula Partners may share employees' and member, clients or suppliers' personal information with authorised third parties as well as obtain information from such third parties for reasons set out above.

4.11.2 Kula Partners may also disclose employees' or member, clients or suppliers' information where there is a duty or a right to disclose in terms of applicable legislation, the law or where it may be necessary to protect the rights of the organisation, or it is in the interests of the data subject.

5. SAFEGUARDING OF PERSONAL INFORMATION AND CONSENT

5.1. Kula Partners will review its security controls and processes on a regular basis to ensure that personal information is secure.

- 5.2. It will take appropriate, reasonable technical and organisational measures to prevent loss or damage or unauthorised destruction of personal information, and unlawful access to or processing of personal information. This will be achieved by:
- Identifying internal and external risks.
 - Establishing and maintaining appropriate safeguards.
 - Regularly verifying these safeguards and their implementation.
 - Updating the safeguards.
 - Implementing generally accepted information security practices and procedures.
- 5.3. Kula Partners will appoint an Information Officer who is responsible for compliance with the conditions of the lawful processing of personal information and other provisions of POPI.
- 5.4. Information Officer details: Johannes Swanepoel
 010 109 1504 / jonie@kulapartners.co.za
 Kaya House Ground Floor
 195 Jan Smuts Avenue
 Parktown North, 2193
- 5.5. The specific responsibilities of the Information Officer include:
- 5.5.1. The development, implementation, monitoring and maintenance of a compliance framework.
- 5.5.2. The undertaking of a personal information impact assessment to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.
- 5.5.3. The development, monitoring and maintenance of a manual, as well as the making available thereof as prescribed in section 51 of PAIA.
- 5.5.4. The development of internal measures, together with adequate systems to process requests for information or access thereto.
- 5.5.5. To ensure that company staff awareness sessions are conducted regarding the provisions of POPI, regulations made in terms of POPI, codes of conduct or information obtained from the Regulator. Accordingly, The Information Officer must maintain evidence of personal information impact assessments, security safeguard reviews, staff awareness and privacy related control testing.
- 5.5.6. Employment contracts and addendums thereto contain relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI are signed by every employee.
- 5.5.7. On an ongoing basis, all suppliers, insurers and other third party service providers are required to sign a service level agreement guaranteeing their commitment to the protection of personal information. Accordingly, service providers that process personal information for Kula Partners must be subject to written operator or security obligations, including confidentiality, breach escalation and return or destruction of information
- 5.5.8. Consent to process client, member or supplier information is obtained from clients, members or suppliers (or a person who has been given authorisation from the client or

member to provide the member or client's personal information) and suppliers at sign-on, appointment or contracting.

6. DIRECT MARKETING

Kula Partners will ensure that:

- 6.1. It does not process any personal information for the purpose of direct marketing (by means of any form of electronic communication, including automatic calling machines, SMSes or e-mail) unless the data subject has given his, her or its consent to the processing or is an existing customer.
- 6.2. It will only approach data subjects, whose consent is required and who have not previously withheld such consent, once to request the consent. This will be done in the prescribed manner and form.
- 6.3. The data subjects will only be approached for the purpose of direct marketing of Kula Partners own similar products or services. In all instances, the data subject will be given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details at the time when the information is collected.
- 6.4. Any communication for the purpose of direct marketing will contain 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 a request that such communications cease.

7. TRANSFER OF INFORMATION OUTSIDE OF SOUTH AFRICA

Kula Partners will not transfer personal information about data subject to a third party who is in a foreign country unless one or more of the following apply:

- 7.1. The third party is subject to a law, binding corporate rules or a binding agreement which provides an adequate level of protection of personal information and effectively upholds principles for reasonable processing of the information.
- 7.2. The data subject consents to the transfer.
- 7.3. The transfer is necessary for the performance of a contract between the data subject and Kula Partners.
- 7.4. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between Kula Partners and a third party.
- 7.5. The transfer is for the benefit of the data subject, and 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.

8. SURVEILLANCE SYSTEMS

Video footage and or telephone calls that have been recorded, processed and stored via security system or other surveillance systems constitutes personal information. As such Kula Partners will make all employees, members, clients or data subjects aware as to the use of security

system and other surveillance on the building.

9. SECURITY BREACHES

- 9.1. Should Kula Partners detect a security breach on any of its systems that contain personal information, it will take the required steps to assess the nature and extent of the breach in order to ascertain if any information has been compromised.
- 9.2. Kula Partners will notify the affected parties should it have reason to believe that their information has been compromised. Such notification will only be made where the organisation can identify the data subject to which the information relates. Where it is not possible it may be necessary to consider website publication and whatever else the Information Regulator prescribes.
- 9.3. Notification will be provided in writing by means of either email, registered mail or Kula Partners's website
- 9.4. The notification will provide the following information where possible description of possible consequences of the breach, measures taken to address the breach, recommendations to be taken by the data subject to mitigate adverse effects, and the identity of the party is responsible for the breach.
- 9.5. In addition to the above, Kula Partners will notify the Regulator of any breach and compromise to personal information in its possession and work closely with and comply with any recommendations issued by the Regulator.
- 9.6. The following will apply in this regard:
 - The Information Officer will be responsible for overseeing the investigation.
 - The Information Officer will be responsible for reporting to the Information Regulator within three working days of a breach or compromise to personal information.
 - The Information Officer will be responsible for reporting to the data subject(s) within three working days, as far as it is reasonable and practicable, of a breach or compromise to personal information.
 - The timeframes above are guidelines and depending on the merits of the situation may require earlier or later reporting.

In conclusion, any suspected or confirmed compromise of personal information must be escalated to the Information Officer for assessment of notification obligations to the Information Regulator and affected data subjects.

10. ACCESS AND CORRECTION OF PERSONAL INFORMATION

- 10.1. Employees and members or clients have the right to request access to any personal information that Kula Partners holds about them.
- 10.2. Employees and members or clients have the right to request Kula Partners to update, correct or delete their personal information on reasonable grounds. Such requests must be made to the Information Officer (see details above) or to Kula Partners office (see details below).
- 10.3. Where an employee or member or client objects to the processing of their personal information, Kula Partners may no longer process said personal information. The

consequences of the failure to give consent to process the personal information must be set out before the employee or client confirms his/her objection.

- 10.4. The member or client or employee must provide reasons for the objection to the processing of his/her personal information.

11. RETENTION OF RECORDS

Kula Partners is obligated to retain certain information as prescribed by law. This includes but is not limited to the following:

- 11.1.1. Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Companies Act 71 of 2008 for a period of seven years.
- 11.1.2. Notice and minutes of all meetings, including resolutions adopted.
- 11.1.3. Copies of reports presented at the annual general meeting.
- 11.1.4. Copies of annual financial statements and copies of accounting records.
- 11.1.5. The Basic Conditions of Employment Act 75 of 1997 requires the organisation to retain records relating to its staff for a period of no less than three years.

12. AMENDMENTS TO THIS POLICY

Amendments to this Policy will take place from time to time subject to the discretion of Kula Partners and pursuant to any changes in the law. Such changes will be brought to the attention of employees, members, and clients where they affect them.

13. REQUESTS FOR INFORMATION

In terms of requests to be processed under POPI, the following forms will be used:

- 13.1. Objection to the processing of personal information – A data subject who wishes to object to the processing of personal information in terms of section 11(3)(a) of POPI.
- 13.2. Request for correction or deletion of personal information or destruction or deletion of record of personal information – A data subject who wishes to request a correction or deletion of personal information or the destruction or deletion of a record of personal information in terms of section 24(1) of POPI.
- 13.3. Request for data subject's consent to process personal information – A responsible party who wishes to process personal information of a data subject for the purpose of direct marketing by electronic communication must submit a request for written consent to that data subject.
- 13.4. Submission of complaint – Any person who wishes to submit a complaint contemplated in section 74(1) of POPI must submit such a complaint to the Regulator on Part I. A responsible party or a data subject who wishes to submit a complaint contemplated in section 74(2) of POPI must submit such a complaint to the Regulator in Part II.

ANNEXURE

LEGISLATIVE MAPPING REGISTER

Policy section or clause	Existing issue or gap identified	Legislative or regulatory source	Required update made	Reason or risk if not updated	Status
9	Breach process required clearer escalation and evidence.	POPIA ss19-22	Inserted security compromise notification assessment clause.	Failure to notify can create regulatory exposure.	Updated
5.5.7	Third-party processing needed stronger operator wording.	POPIA ss20-21	Inserted operator/security obligations.	Outsourced processing creates privacy risk.	Updated
5.5	Evidence of PI impact assessments and awareness needed strengthening.	POPIA Regulation 4; governance	Inserted evidence maintenance clause.	Supports Information Officer accountability.	Updated