Registration Number of Company: 2014/041495/07

**JINJA 2 OUTDOOR ADVERTISING (PTY) LTD**

**POPI MANUAL**

**COMPLIANCE MANUAL FOR**

**THE IMPLEMENTATION OF THE**

**PROTECTION OF PERSONAL INFORMATION ACT**

**NO 4 OF 2013**

**(POPIA)**

DATE OF COMPILATION: JUNE 2021
DATE OF REVISION: JUNE 2021

# INDEX

## 1. INTRODUCTION

The Protection of Personal Information Act (POPIA) is intended for competing interests. These are:

1.1. Constitutional rights to privacy for individuals (personal information to be protected); and

1.2. The needs of society to have access to and to process (work with) personal information for legitimate purposes, including the purpose of doing business.

Personal information means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.

This POPI Manual sets out the framework for the company's compliance with POPI.
Where reference is made to the "processing" of personal information, it means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information.

## 2. UNDERTAKING TO CLIENTS

2.1. The company undertakes to follow POPI at all relevant times and to process personal information lawfully and reasonably, so as not to infringe unnecessarily on the privacy of clients.

2.2. The company undertakes to process information only for the purpose for which it is intended, to enable the company to do our work, as agreed with clients.

2.3. Whenever necessary, the company shall obtain consent to process personal information.

2.4. Where the company does not seek consent, the processing of the company's client's personal information will be following a legal obligation placed upon the company, or to protect a legitimate interest that requires protection.

2.5. The company shall stop processing personal information if the required consent is withdrawn, or if a legitimate objection is raised.

2.6. The company shall collect personal information directly from the client whose information the company require, unless:

2.6.1. the information is of public record, or

2.6.2. the client has consented to the collection of their personal information from another source, or

2.6.3. the collection of the information from another source does not prejudice the client, or

2.6.4. the information to be collected is necessary for the maintenance of law and order of national security, or

2.6.5. the information is being collected to comply with a legal obligation, including an obligation to SARS, or

2.6.6. the information collected is required for the conduct of proceedings in any court of tribunal, where these proceedings have commenced or are reasonably contemplated, or

2.6.7. the information is required to maintain the company legitimate interests, or

2.6.8. where requesting consent would prejudice the purpose of the collection of the information, or

2.6.9. where requesting consent is not reasonably practical in the circumstances.

2.7. The company shall advice its clients of the purpose of the collection of the personal information.

2.8. The company will retain records of the personal information the company has collected for the minimum period as required by law unless the client has furnished their consent or instructed us to retain the records for a longer period.

2.9. The company will destroy or delete records of the personal information (to de-identify the client) as soon as reasonably possible, after the period for which the company were entitled to hold the records have expired.

2.10. We will restrict the processing of personal information:

2.10.1. where the accuracy of the information is contested, for a period sufficient to enable us to verify the accuracy of the information;

2.10.2. where the purpose for which the personal information was collected has been achieved and where the personal information is being retained only for the purposes of proof;

2.10.3. where the client requests that personal information is not destroyed or deleted, but rather retained; or

2.10.4. where the client requests that the personal information be transmitted to another automated data processing system.

2.11. The further processing of personal information will only be undertaken:

2.11.1. if the requirements of paragraphs 2.3, 2.6.1, 2.6.4, 2.6.5 or 2.6.6 above have been met;

2.11.2. where further processing is necessary because of a threat to public health or public safety or to the life or health of the client, or a third person;

2.11.3. where the information is used for historical, statistical or research purposes and the identity of the client will not be disclosed; or

2.11.4. where this is required by the Information Regulator appointed in terms of POPI

2.12. The company undertakes to ensure that the personal information which the company collects and process is complete, accurate, not misleading and up-to-date.

2.13. The company undertakes to retain the physical file and the electronic date related to the processing of the personal information.

2.14. The company undertakes to take special care with the company's client's bank account details, and the company is not entitled to obtain or disclose or procure the disclosure of such banking details unless the company has the client's specific consent.

.

## 3. CLIENT'S RIGHTS

3.1. In cases where the client's consent is required to process their personal information, this consent may be withdrawn.

3.2. In cases where the company processes personal information without consent to protect a legitimate interest, to comply with the law or to pursue or protect our legitimate interests, the client has the right to object to such processing.

3.3. All clients are entitled to lodge a complaint regarding the company's application of POPI with the Information Regulator.

3.4. The prescribed forms for the exercise of these rights are provided in the schedule to this POPI Manual.

## 4. SECURITY SAFEGUARDS

4.1. To secure the integrity and confidentiality of the personal information in our possession, and to protect it against loss or damage or unauthorised access, the company must continue to implement the following security safeguards:

4.1.1. The business premises where records are kept must remain protected by access control, alarms and armed response.

4.1.2. All the user terminals on the internal computer network and the servers must be protected by only giving authorised personnel access to them.
4.1.3. The email infrastructure must comply with industry standard security safeguards, including passwords that is updated regularly.
4.1.4. Vulnerability assessments must be carried out on our digital infrastructure on an annual basis to identify weaknesses in the company system and to ensure the company has adequate security in place.
4.1.5. Archived files must be stored behind locked doors and access control to these storage facilities must be implemented.
4.1.6. Firewall software and Anti-malware software protects the data on the local servers. The company must run antivirus at least once a week to ensure the systems are updated with the latest patches.
4.1.7. The staff is trained to carry out their duties in compliance with POPI and this training must be ongoing.
4.1.8. Signed policies must be in place that every staff member maintains full confidentiality in respect of all the client's affairs, including the client's personal information.
4.1.9. Signed policies must be in place that staff whose duty it is to process a client's personal information, must include an obligation on the staff member to
1) maintain the company's security measures, and
2) notify their manager immediately if there are reasonable grounds to believe that the personal information of a client has been accessed of acquired by any unauthorised person.
4.1.10. The processing of the personal information of the staff members must take place in accordance with the rules contained in the relevant labour legislation.
4.1.11. The digital work profiles and privileges of staff who have left the employment must be properly terminated.
4.1.12. The personal information of clients and staff must be destroyed timeously in a manner that de-identifies the person.

4.2. These security safeguards must be verified on a regular basis to ensure effective implementation and these safeguards must be continually updated in response to new risks and weaknesses.

## 5. SECURITY BREACHES

5.1. Should it appear that the personal information of a client has been accessed or acquired by an unauthorised person, personnel must notify the Information Regulator and the relevant client, unless there are no longer information to identify the client. This notification must take place as soon as reasonably possible.

5.2. Such notification must be given to the Information Regulator first as it is possible that they, or another public body, might require the notification to the client be delayed.

5.3. The notification to the client must be communicated in writing in one of the following ways, with a way to ensure that the notification reaches the client:
5.3.1. by mail to the client's last known physical or postal address;
5.3.2. by email to the client's last known email address;
5.3.3. by publication on the website or in the news media; or
5.3.4. as directed by the Information Regulator.

5.4. This notification to the client must give sufficient information to enable the client to protect themselves against the potential consequences of the security breach and must include:
5.4.1. a description of the possible consequences of the breach;
5.4.2. details of the measures that we intend to take or have taken to address the breach;
5.4.3. the recommendation of what the client could do to mitigate the adverse effects of the breach; and
5.4.4. if known, the identity of the person who may have accessed, or acquired the personal information.

## 6. CLIENTS REQUESTING RECORDS

6.1. On production of proof of identity, any person is entitled to request that the company confirm, free of charge, whether or not, the company holds any personal information about that person in their records.

6.2. If we hold such personal information, on request, and upon payment of a fee of R750,00 plus VAT, we shall provide the person with the record, or a description of the personal information, including information about the identity of all third parties or categories of third parties who have or have had access to the information. We shall do this within a reasonable period, in a reasonable manner and in an understandable form.

6.3. A client requesting such personal information must be advised of their right to request to have any errors in the personal information corrected, which request shall be made on the prescribed application form.

6.4. In certain circumstances, we will be obliged to refuse to disclose the record containing the personal information to the client. In other circumstances, we will have discretion as to whether or not to do so.

6.5. In all cases where the disclosure of a record will entail the disclosure of information that is additional to the personal information of the person requesting the record, the written consent of the Information Officer, or his delegate, will be required and that person will make their decision having regard to the provisions of Chapter 4 of Part 3 of the Promotion of Access to Information Act.

6.6. If a request for personal information is made and part of the requested information may, or must be refused, every other part must still be disclosed.

## 7. THE CORRECTION OF PERSONAL INFORMATION

7.1. A client is entitled to require to correct or delete personal information that the company has, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or which has been obtained unlawfully.

7.2. A client is entitled to require us to destroy or delete records of personal information about the client that we are no longer authorised to retain.

7.3. Any such request must be made on the prescribed form.

7.4. Upon receipt of such lawful request, we must comply as soon as reasonably practical.

7.5. If a dispute arises regarding the client’s rights to have information corrected, and if the client so requires, we must attach to the information, in a way that it will always be read with the information, an indication that the correction of the information has been requested but has not been made.

7.6. We must notify the client who has made a request for their personal information to be corrected or deleted, what action we have taken as a result of such request.

## 8. SPECIAL PERSONAL INFORMATION

8.1. Special rules apply to the collection and use of information relating to a person's religious or philosophical beliefs, their race or ethnic origin, their trade union membership, their political persuasion, their health or sex life, their biometric information, or their criminal behaviour.

8.2. We will not process any of this Special Personal Information without the client's consent, or where it is necessary for the establishment, exercise or defence of a right or an obligation in law.

8.3. It is unlikely that we will ever have to process special personal information, due to the nature of our business, but should it be necessary the guidance of the Information Officer, or his delegate, must be sought.

## 9. THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN

The company may only process the personal information of a child if we have the consent of the child's parent or legal guardian.

## 10. INFORMATION OFFICER

10.1. Our Information Officer is designated to be Martin Raubenheimer. The Information Officer may delegate his authority to a senior staff member or manager. The Information Officer's duties and responsibilities include:
10.1.1. Ensuring compliance with POPI Act
10.1.2. Dealing with requests which we receive in terms of POPI Act
10.1.3. Working with the Information Regulator in relation to investigations.

10.2. The Information Officer must designate in writing as many Deputy Information Officers as necessary to perform the tasks in paragraph 1.

10.3. The Information Officer and Deputy Information Officer must register with the Information Regulator prior to taking up their duties.

10.4. In carrying out his duties, the Information Officer must ensure that:
10.4.1. the compliance manual is developed, implemented, monitored, maintained and made available;
10.4.2. a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
10.4.3. internal measures are developed together with adequate systems to process requests for information or access to information;
10.4.4. internal awareness sessions are conducted regarding the provisions of POPIA, the Regulations, codes of conduct or information obtained from the Information Regulator; and
10.4.5. copies of this manual are provided to persons at their request, upon payment of a fee to be determined by the Information Regulator.

## 11. CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION

11.1. In the following circumstances, the company will require prior authorization from the Information Regulator before processing any personal information:

11.1.1. In the event that the company intends to utilize any unique identifiers of clients (account numbers or other numbers or codes allocated to clients for the purpose of identifying them in our business) for any purpose other that the original intention, or to link the information with information held by others;

11.1.2. If the company is processing information on criminal behavior or unlawful or objectionable conduct;

11.1.3. If the company is processing information for the purposes of credit reporting;

11.1.4. If the company is transferring special personal information or the personal information of children to a third party in a foreign country, that does not provide adequate protection of that personal information.

11.2. The Information Regulator must be notified of our intention to process any personal information as set out in paragraph 11.1.1 prior to any processing taking place and we may not commence with such processing until the Information Regulator has decided in our favour. The Information Regulator has 4 weeks to decide but may decide that a more detailed investigation is required. In this event the decision must be made in a period as indicated by the Information Regulator, which must not exceed 13 weeks. If the Information Officer does not decide within the stipulated time periods, we can assume that the decision is in our favour and commence processing the information.

## 12. DIRECT MARKETING

12.1. The company may only carry out direct marketing (using any form of electronic communication) to clients if:

12.1.1. they were given an opportunity to object to receiving direct marketing material by electronic communication at the time that their personal information was collected; and

12.1.2. they did not object then or at any time after receiving any such direct marketing communications from us.

12.2. We may only approach clients using their personal information, if we have obtained their personal information in the context of our normal services to them, and we may then only market our normal services to them.

12.3. We may only carry out direct marketing (using any form of electronic communication) to other people if we have received their consent to do so.

12.4. We may approach a person to ask for their consent to receive direct marketing material only once, and we may not do so if they have previously refused their consent.

12.5. A request for consent to receive direct marketing must be made in the prescribed manner and form. The prescribed form of this request and consent is an annexure to this compliance manual.

12.6. All direct marketing communication must disclose our identity and contain an address or other contact details to which the client may send a request that the communications cease.

## 13. TRANSBORDER INFORMATION FLOWS

13.1. The company may not transfer a client's personal information to a third party in a foreign country, unless:

13.1.1. the client consents to this, or requests it; or

13.1.2. such third party is subject to a law, binding corporate rules or a binding agreement which protects the personal information in a manner like POPIA, and such third party is governed by similar rules which prohibit the onward transfer of the personal information to a third party in another country; or

13.1.3. the transfer of the personal information is required for the performance of the contract between the company and the client; or

13.1.4. the transfer is necessary for the conclusion or performance of a contract for the benefit of the client entered into between the company and the third party; or

13.1.5. the transfer of the personal information is for the benefit of the client, and it is not reasonably possible to obtain their consent and that if it were possible the client would be likely to give such consent.

## 14. CURTAILMENT OF POWERS OF SEARCH AND SEIZURE (PROFESSIONAL PRIVILEGE)

14.1. The powers of search and seizure conferred by search warrant issued at the request of the Information Regulator must be exercised in respect of any communication between the company and our clients in connection with the giving of legal advice to the client with respect to their obligations, liabilities, or rights or any communications made in connection with or in contemplation of proceedings under or arising out of POPI.

14.2. In the event that would raise the point of privileged information during a search and seizure operation, the person executing the warrant may request that the registrar of the High Court attach and remove that article or document for safe custody until a court of law has made a ruling on the question of privilege.

## 15. OFFENCES AND PENALTIES

15.1. POPI provides for serious penalties for the contravention of its terms. For minor offences, a guilty party can receive a fine or be imprisoned for up to 12 months. For serious offences, the period of imprisonment rises to a maximum of 10 years. Administrative fines for the company can reach a maximum of R10 million. Breaches of this compliance manual will also be viewed as a serious disciplinary offence.

15.2. It is therefore imperative that the company complies strictly with the terms of this POPI Manual and protect the client's personal information in the same way as if it was the company's.

## 16. SCHEDULE OF ANNEXURES AND FORMS

1. PAIA Manual
2. Objection to the processing of personal information (form 1 of the regulations)
3. Request for correction or deletion or personal information (form 2 of the regulations)
4. Application for consent to direct marketing (form 4 of the regulations)

Registration Number of Company: 2014/041495/07

# JINJA 2 OUTDOOR ADVERTISING (PTY) LTD

# PAIA MANUAL

**IN TERMS OF**

**SECTION 51 OF THE**

**PROMOTION OF ACCESS TO INFORMATION ACT**

**ACT 2/2000**

**("THE ACT")**

DATE OF COMPILATION: JUNE 2021
DATE OF REVISION: JUNE 2021

# INDEX

## 1. INTRODUCTION

Jinja 2 Outdoor Advertising is a boutique outdoor advertising outfit, specializing in unlocking and developing billboard opportunities for the joint benefit of its landlords, joint venture partners and itself.

We are a billboard company, which is constantly growing, warranting excellent visibility and exposure to our advertisers, as our primary rationale and focus-billboards and outdoor advertising.

## 2. COMPANY DETAIL [S51(1)(a)]

| | |
|---|---|
| Directors: | Mr. EP Vorster<br>Mr. WM Raubenheimer<br>Mr. WJG Landman<br>Mr. WFC Arndt |
| Managing Director: | Mr. WM Raubenheimer |
| Postal Address: | P.O. Box 32566, Menlo Park, Pretoria, 0102 |
| Registered Address: | Summit Place Building 4, 2nd Floor, 221 Garsfontein Road, Pretoria, 0081 |
| Contact Number: | 076 177 0249 |
| Email: | martin@jinjaoutdoor.co.za |

## 3. THE ACT AND SECTION 10 GUIDE [S51(1)(b)]

The ACT grants a requester access to records of a private body, if the record is required for the exercise or protection of any rights. If a public body lodges a request, the public body must be acting in the public interest. Requesters are referred to the Guide in terms of Section 10 which has been compiled by the South African Human Rights Commission, which will contain information for the purposes of exercising Constitutional Rights. The Guide is available from the South Africa Human Rights Commission.

The South Africa Human Rights Commission:

| | |
|---|---|
| PAIA Unit | |
| Postal Address: | Private Bag 2700, Houghton, 2041 |
| Telephone Number: | +27-11-877 3600 |
| Fax Number: | +27-11-403 0625 |
| Website: | www.sahrc.org.za |

## 4. APPLICABLE LEGISLATION [S51(1)(c)]

| No | Ref | Act |
|---|---|---|
| 1 | No 61 of 1973 | Companies Act |
| 2 | No 95 of 1967 | Income Tax Act |
| 3 | No 89 of 1991 | Value Added Tax Act |
| 4 | No 66 of 1995 | Labour Relations Act |
| 5 | No 75 of 1997 | Basic Conditions of Employment Act |
| 6 | No 25 of 2002 | Electronic Communications and Transactions Act |
| 7 | No 30 of 1996 | Unemployment Insurance Act |
| 8 | No 28 of 2011 | Tax Administration Act |
| 9 | No 2 of 2000 | Promotion of Access of Information Act |
| 10 | No 4 of 2013 | Protection of Personal Information Act |
| 11 | No 130 of 1993 | Compensation for Occupational Injuries and Diseases Act |
| 12 | No 97 of 1998 | Skills Development Act 97 of 1998 |

## 5. SCHEDULE OF RECORDS [S51(1)(d)]

| Record | Subject | Availability |
|---|---|---|
| Incorporation records | Memorandum of Incorporation | Request in terms of PAIA |
| | Company registration records | |
| | Share registers | |
| | Minutes of Board of Directors meeting | |
| Financial records | Financial Statements | |
| | Financial and Tax records | Not available in terms of PAIA |
| | Asset register | |
| | Management Accounts | |
| Other | Minutes of sales meetings | |
| | Advertiser rental agreements | |
| | Landlord Rental agreements | Request in terms of PAIA |
| | Joint Venture agreements | |
| | Employment Contracts | |

## 6. FORM OF REQUEST [S51(1)(e)]

To facilitate the processing of your request, kindly:

6.1. Use the prescribed form, available on the website of the South African Human Rights Commission at www.sahrc.org.za

6.2. Address your request to the CEO of the company.

6.3. Provide sufficient details to enable the Company to identify:

a) The records requested;
b) The requester (and if an agent is lodging the request, proof of capacity);
c) The form or access required;
d) (i) The postal address or fax number of the requester in the Republic;
(ii) If the requester wishes to be informed of the decision in any manner, the manner and particulars thereof

e) The right which the requester is seeking to exercise or protect with an explanation or the reason the record is required to exercise or protect the right.

## 7. PRESCRIBED FEES [S51(1)(f)]

The following applies to request (other than personal requests):

7.1. A requester is required to pay the prescribed fees (R50.00);
7.2. If the preparation of the record requested requires more than the prescribed hours (six), a deposit shall be paid (of not more than one third of the access fee which would be payable if the request were granted;
7.3. A requestor may lodge an application with a court against the tender/payment of the request fee and/or deposit;
7.4. Records may be withheld until fees have been paid;
7.5. The fee structure is available on the website of the South African Rights Commission at www.sahrc.org.za