POLICY STATEMENT AND MANUAL

PROTECTION OF PERSONAL INFORMATION AND THE RETENTION OF DOCUMENTS

FOR

SIGNMAN CC

(Registration No.: 1989/008690/23)

(hereinafter referred to as "SIGNMAN")

Last Updated: July 2021

INDEX

A: PROTECTION OF PERSONAL INFORMATION IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT, NO. 4 OF 2013

1 INTRODUCTION

1.1 SIGNMAN has been operating since 1975 as a specialist in the design, manufacturing and installation of signs of a variety of nature and size, and is a household name in the signage industry nationally. The client base of SIGNMAN is diverse, and include but are not limited to, the retail and banking sectors. Part of the showcase of signage offered by SIGNMAN is SmartPole, a unique modular sign system offering a wide range of outdoor solutions in a compact design.

1.2 SIGNMAN is required to comply with the relevant provisions of the Protection of Personal Information Act, No. 4 of 2013 ("POPI"). POPI requires SIGNMAN to inform its clients as to the manner in which their personal information is used, disclosed and destroyed.

1.3 SIGNMAN commits to protecting its clients', contractors' and service providers' privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

1.4 Its Policy sets out the manner in which SIGNMAN deals with its clients', contractors' and service providers' personal information, and stipulates the purpose for which such information is used. The Policy is accessible on the SIGNMAN company website www.signman.co.za and by written request to the Information Officer.

1.5 Where applicable, the provisions of this Policy shall also apply to personal information of employees of SIGNMAN.

2 PURPOSE OF POPI

The purpose of POPI is to:

2.1 Give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations which are aimed at –

(a) balancing the right to privacy against other rights, particularly the right of access to information; and

(b) protecting important interests, including the free flow of information within South Africa and across international borders.

2.2 Regulates the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, which prescribe the minimum threshold requirements for the lawful processing of personal information.

2.3 Provide persons with rights and remedies to protect their personal information from processing which is not in accordance with POPI.

2.4 Establish voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by POPI.

3 APPLICATION AND INTERPRETATION OF POPI

POPI applies to processing of personal information:

3.1 Entered into a record by or for a responsible party by making use of automated or non-automated means, provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof.

3.2 Where the responsible party is domiciled in South Africa or not domiciled in South Africa, but makes use of automated or non-automated means in South Africa, unless those means are used only to forward personal information through South Africa.

3.3 Subject to paragraph 3.2 above, to the exclusion of any provision of any other legislation which regulates the processing of personal information and which is materially inconsistent with an object or a specific provision of POPI. If any other legislation provides for conditions for the lawful processing of personal information which are more extensive, such extensive conditions shall prevail.

4 IMPORTANT DEFINITIONS

4.1 **‘automated means’** – in application to paragraph 3 above, means any equipment capable of operating automatically in response to instructions given for the purpose of processing information;

4.2 **‘binding corporate rules’ –** means personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country;

4.3 **‘biometrics’** – means a technique of personal identification which is based on physical, physiological or behavioral characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;

4.4 **‘consent’** – means permission given for the processing of personal information;

4.5 **'data subject'** - means the person to whom personal information relates;

4.6 **'de-identify'** - in relation to personal information of a data subject, means to delete any information which can identify, be used/manipulated to identify a data subject or can be linked to other information which identifies the data subject;

4.7 **'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;

4.8 **'filing system'** - means any structured set of personal information which is accessible according to specific criteria;

4.9 **‘group of undertakings’ –** means a controlling undertaking and its controlled undertakings;

4.10 **‘information officer’** – means in relation to a public body, an information officer or deputy information officer contemplated in terms of section 1 or 17 of the Promotion of Access to Information Act, No. 2 of 2000 (“PAIA”), and in relation to a private body, means the head of a private body as contemplated in section 1 of PAIA;

4.11 **‘operator’** - means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

4.12 **'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 –

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical/mental health, wellbeing, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

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

(d) biometric information of the person;

(e) personal opinions, views or preferences of the person;

(f) correspondence sent by the person which is implicitly or explicitly of a private or confidential nature, or further correspondence which would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) 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;

4.13 **'private body'** – means -

(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;

(b) a partnership which carries on or has carried on any trade, business or profession; or

(c) any former or existing juristic person, but excludes a public body;

4.14 **'processing'** - means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –

(a) collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by transmission, distribution or making available in any form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;

4.15 **'public body'** – means –

(a) any department of State or administration in the national or provincial sphere of government, or any municipality in the local sphere of government; or

(b) any other functionary or institution when exercising a power or performing a duty in terms of the Constitution or a provincial constitution, or exercising a public power or performing a public function in terms of any legislation;

4.16 **'record'** - means any recorded information regardless of form or medium, in the possession or under the control of a responsible party, whether or not it was created by a responsible party, and regardless of when it came into existence;

4.17 **'Regulator'** - means the information regulator established in terms of section 39 of POPI;

4.18 **'responsible party'** - means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

4.19 **'special personal information'** – means –

(a) 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

(b) 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.

5 CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

POPI provides for eight conditions for the lawful processing of personal information, which appear hereunder, with reference to the particular sections of POPI, *viz:*

5.1 **Condition 1: Accountability** (section 8);

5.2 **Condition 2: Processing limitation** (sections 9 to 12);

5.3 **Condition 3: Purpose specification** (sections 13 and 14);

5.4 **Condition 4: Further processing limitation** (section 15);

5.5 **Condition 5: Information quality** (section 16);

5.6 **Condition 6: Openness** (sections 17 and 18);

5.7 **Condition 7: Security safeguards** (sections 19 to 22); and

5.8 **Condition 8: Data subject participation** (sections 23 to 25).

6 PERSONAL INFORMATION COLLECTED

6.1 **Section 10** of POPI states that "*Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.*"

6.2 SIGNMAN collects and processes clients', contractors' and service providers' personal information. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Whenever possible, SIGNMAN will inform clients, contractors and service providers as to the information required and the information deemed optional. Examples of personal information SIGNMAN collects include, but are not limited to:

a) Description of clients', contractors' and service providers' business, assets, financial information,banking details, trade connections, etc; and

b) Any other information required by SIGNMAN in order to enable it to provide the logistics services solutions to clients.

6.3 SIGNMAN also collects and processes clients' personal information for marketing purposes in order to ensure that its products and services remain relevant to its clients and potential clients.

6.4 SIGNMAN aims to procure written agreements with all contractors, suppliers, insurers and other third party service providers to ensure a mutual understanding with regard to the protection of clients' personal information. SIGNMAN's contractors, insurers and other third party service providers will be subject to the same regulations as applicable to SIGNMAN.

6.5 For purposes of this Policy, clients include potential and existing clients.

6.6 Client information shall be obtained by SIGNMAN from a person duly authorised to provide and/or authorise the provision of such information of a client, contractor and service provider to SIGNMAN.

7 THE USE OF PERSONAL INFORMATION

7.1 Personal information will only be used for the purpose for which it was collected and as may be agreed, which may include but are not limited to:

(a) Providing services to clients and to carry out the transactions requested;

(b) Conducting credit reference searches or verification;

(c) Confirming, verifying and updating client, contractor and service provider details;

(d) Detection and prevention of fraud, crime, money laundering or other malpractices;

(e) Conducting market or customer satisfaction research;

(f) Audit and record keeping purposes;

(g) In connection with legal proceedings;

(h) Providing SIGNMAN requested services to clients, and to maintain and constantly improve the relationship;

(i) Providing communication in respect of SIGNMAN and regulatory matters which may affect clients; and

(j) In connection with and to comply with legal and regulatory requirements or when it is otherwise required by law.

7.2 According to section 11 of POPI, personal information may only be processed if certain conditions listed below are met:

(a) Clients', contractors' and service providers' consent to the processing. Consent is obtained from clients, contractors and service providers during the introductory, appointment and needs analysis stage of the relationship;

(b) The necessity of processing in order to conduct an accurate analysis of clients' needs for purposes of amongst other credit applications, insurance requirements, service delivery needs, etc;

(c) Processing complies with an obligation imposed by law on SIGNMAN, e.g. rules and regulations imposed by the Financial Intelligence Centre Act, No. 38 of 2001, as amended ("FICA") and its regulations;

(d) Processing is necessary in order to protect the interests of clients by providing for protection measures in respect of the personal information of clients in the service delivery supply chain;

(e) Processing is necessary to ensure the proper performance of a public law duty by a public body, including but not limited to, with reference to customs and excise; and

(f) Processing is necessary for pursuing the legitimate interests of SIGNMAN or of any third party engaged by it in the service delivery supply chain to promote optimal service delivery to clients and protection of their personal information.

8 DISCLOSURE OF PERSONAL INFORMATION

8.1 SIGNMAN may disclose clients' personal information to any of SIGNMAN group companies or subsidiaries, joint venture companies and or approved third party service providers reasonably required to perform the required services to clients. SIGNMAN has agreements in place to ensure compliance with confidentiality and privacy conditions.

8.2 SIGNMAN may also disclose clients' information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect the rights of SIGNMAN.

9 SAFEGUARDING CLIENT INFORMATION

9.1 It is a requirement of POPI to adequately protect personal information. SIGNMAN will continuously review its security controls and processes to ensure that personal information is secured.

9.2 The following procedures are utilised in order to protect personal information:

9.2.1 The Information Officer is responsible for compliance with the conditions of the lawful processing of personal information and other provisions of POPI, and will be assisted by other designated personnel;

9.2.2 This Policy has been implemented throughout SIGNMAN, and training on this Policy and POPI has taken place. Training records are duly recorded and retained;

9.2.3 New employees will be required to sign written particulars of employment containing relevant consent clauses for the use and storage of employee information or any other action so required in terms of POPI, and will receive relevant POPI training;

9.2.4 Where applicable, employees currently employed by SIGNMAN will be required to sign an addendum to their written particulars of employment containing relevant consent clauses for the use and storage of employee information or any other action so required in terms of POPI;

9.2.5 Client information is archived and stored by SIGNMAN on site, and access thereto is restricted to designated personnel. SIGNMAN shall ensure that electronic files or data are backed up, and shall ensure that duly qualified and experienced information technology personnel or service providers are engaged to procure and maintain system security, amongst other, to provide the protection and safeguarding of personal information;

9.2.6 Contractual documents entered into by SIGNMAN and third party service providers engaged in delivering the required services to clients shall contain apposite clauses committing such service providers to comply with POPI;

9.2.7 All electronic files or data are backed up by the information technology department which is also responsible for system security which protects third party access and physical threats. The information technology department is responsible for electronic information security.

10 ACCESS AND CORRECTION OF PERSONAL INFORMATION

Clients, contractors and service providers have the right to access their personal information held by SIGNMAN. Clients, contractors and service providers also have the right to request in writing for SIGNMAN to update, correct or delete their personal information on reasonable grounds. Once a client objects to the processing of its personal information, SIGNMAN may no longer process the said personal information unless it is reasonably required to do so by SIGNMAN in order to fulfil its contractual obligations pursuant to its services contracted to the client. SIGNMAN shall effect changes, updates and the cessation of use of personal information from clients, contractors and service providers only upon receipt of written request to do so from a duly authorised person.

11 DETAILS OF INFORMATION OFFICER/S AND HEAD OFFICE

11.1 INFORMATION OFFICER DETAILS

NAME: DESMOND GOBEY

TELEPHONE NUMBER: 011 493 0146

FAX NUMBER: N/A

E-MAIL ADDRESS: des@signman.co.za

11.2 DEPUTY INFORMATION OFFICER DETAILS

NAME: MART-MARIE VAN HEERDEN

TELEPHONE NUMBER: 011 493 0146

FAX NUMBER: N/A

E-MAIL ADDRESS: mart@signman.co.za

11.3 **HEAD OFFICE DETAILS**

TELEPHONE NUMBER: 011 493 0146

FAX NUMBER: N/A

E-MAIL ADDRESS: des@signman.co.za

POSTAL ADDRESS: Postnet Suite 096
Private Bag X10010
Edenvale
1610

PHYSICAL ADDRESS: 32 Stevens Road, Stafford, Johannesburg, 2000

WEBSITE: www.signman.co.za

11.4 **DUTIES AND RESPONSIBILITIES OF INFORMATION OFFICER**

11.4.1 The Information Officer will take up his/her duties in terms of POPI once he/she has been registered by SIGNMAN with the Regulator.

11.4.2 The Information Officer's responsibilities shall include –

(a) the encouragement of compliance by SIGNMAN with the conditions for the lawful processing of personal information;

(b) dealing with requests made to SIGNMAN pursuant to POPI;

(c) working with the Regulator in relation to investigations conducted pursuant to chapter 6 of POPI in relation to SIGNMAN;

(d) otherwise ensuring compliance by SIGNMAN with the provisions of POPI; and

(e) any other responsibilities as may be prescribed.

11.4.3 SIGNMAN shall make provision as prescribed in section 17 of PAIA for such number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities set out in paragraph 11.4.2 above, and any power or duty conferred or imposed on an information officer by POPI to a

deputy information officer of SIGNMAN.

12 PAIA INTERACTION

12.1 The objects of PAIA are to give effect to the constitutional right of access to any information held by the State and any information which is held by another person and which is required for the exercise or protection of any rights.

12.2 Part 3 of PAIA deals with the access to records of private bodies.

12.3 Section 51 of PAIA requires of the head of a private body to compile a manual with particular required information contained therein, and must update such manual regularly. Such manual must be made available on the website of the private body, at the principal place of business of the private body and to any person upon request and upon the payment of a reasonable amount, as well as to the Information Regulator upon request.

12.4 The head of a private body, which is a juristic body, is the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer or the person who is acting as such or any person duly authorised by such acting person.

12.5 If a request is made to SIGNMAN for access to a record (information), it must be made in the prescribed form as referred to in section 53 of PAIA, and in terms of section 54 thereof, the requesting party is liable to pay the prescribed request fee before the processing of the request.

12.6 If a request for a record is received and such record cannot be found or do not exist, SIGNMAN must deal with such matter as prescribed by section 55 of PAIA.

12.7 Sections 63 to 67 of PAIA provide for the mandatory protection of privacy/information of various third parties and other instances, and section 69 provides for the mandatory protection of research information of a third party and of SIGNMAN.

12.8 Section 68 of PAIA provides grounds for the refusal by SIGNMAN to provide certain information sought by a requester.

13 AMENDMENTS TO THIS POLICY

Amendments to, or a review of this Policy will take place on an *ad hoc* basis or at least once a year. Clients are advised to access SIGNMAN's website periodically to keep abreast of any changes. Where material changes take place, clients, contractors and service providers will be notified directly.

14 AVAILABILITY OF THIS POLICY AND THE PAIA MANUAL

Copies of this Policy and the prescribed PAIA manual are available on the website of SIGNMAN and at its head office, and available to the Information Regulator upon request.

END

B: POLICY ON THE RETENTION & CONFIDENTIALITY OF DOCUMENTS, INFORMATION AND ELECTRONIC TRANSACTIONS

1. PURPOSE

1.1 To exercise effective control over the retention of documents and electronic transactions:

1.1.1 as prescribed by legislation; and

1.1.2 as dictated by business practice.

1.2 Documents are required to be retained in order to prove the existence of facts and in order to exercise rights SIGNMAN may have. Documents are also necessary for defending legal action, for establishing what was recorded or performed in relation to business of SIGNMAN and to minimize its reputational risks.

1.3 To ensure that SIGNMAN's interests are protected and that its andclients' rights to privacy and confidentiality are not infringed upon.

1.4 Queries may be referred to the Information Officer.

2. SCOPE & DEFINITIONS

2.1 All documents and electronic transactions generated within and/or received by SIGNMAN fall within the scope.

2.2 **Definitions**

2.2.1 **'clients'** include, but are not limited to, clients of SIGNMAN, contractors, service providers, shareholders, debtors, creditors as well as the affected personnel and/or departments related to a service division of SIGNMAN.

2.2.2 **'confidential information'** refers to all information or data disclosed to or obtained by SIGNMAN by any means whatsoever and shall include, but not be limited to:

(a) financial information and records; and

(b) all other information, including information relating to the structure, operations, processes, intentions, business information, know-how, trade secrets, market opportunities, customers and business affairs, but excluding the exceptions listed in clause 3.1 hereinbelow.

2.2.3 **'Constitution'** means the Constitution of the Republic of South Africa, Act 108 of 1996.

2.2.4 **'data'** refers to electronic representations of information in any form.

2.2.5 **'documents'** include books, records, security or accounts and any information which have been stored or recorded electronically, photographically, magnetically, mechanically, electro-mechanically or optically, or in any other form.

2.2.6 **'ECTA'** means the Electronic Communications and Transactions Act, No. 25 of 2002.

2.2.7 **'electronic communication'** refers to a communication by means of data messages.

2.2.8 **'electronic signature'** refers to data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature.

2.2.9 **'electronic transactions'** include e-mails sent and received.

2.2.10 **'PAIA'** means the Promotion of Access to Information Act, No. 2 of 2000.

3. ACCESS TO DOCUMENTS

3.1 All SIGNMAN and client information must be dealt with in the strictest confidence and may only be disclosed, without fear of redress, in the following circumstances (also see clause 3.2 below):

3.1.1 where disclosure is under compulsion of law;

3.1.2 where there is a duty to the public to disclose;

3.1.3 where the interests of SIGNMAN require disclosure; and

3.1.4 where disclosure is made with the express or implied consent of the client.

3.2 Disclosure to third parties:

All employees have a common law and/or contractual duty of confidentiality in relation to SIGNMAN and its clients. In addition to the provisions of clause 3.1 above, the following are also applicable:

3.2.1 **Information on clients:** Clients' rights to confidentiality are protected in terms of the Constitution and in terms of ECTA. Information may be given to a third party if a client has consented in writing to such person receiving the information.

3.2.2 **Requests for SIGNMAN information:**

3.2.2.1 Such requests are dealt with in terms of PAIA, which gives effect to the constitutional right of access to information held by the State or any person (natural and juristic) which is required for the exercise or protection of rights. Private bodies, such as SIGNMAN must however refuse access to records if disclosure may constitute a breach of the duty of secrecy owed to a third party.

3.2.2.2 Requests for information must be made in writing on the prescribed form to the Information Officer in terms of PAIA. The requesting party has to state the reason for requesting the information and has to pay a prescribed fee.

3.2.2.3 SIGNMAN's manual in terms of PAIA, which contains the prescribed forms and details of prescribed fees, is available on the intranet and its website www.SIGNMAN.co.za

3.2.3 Confidential company and/or business information of SIGNMAN may not be disclosed to third parties without due authorisation from the Information Officer. The business and financial affairs of SIGNMAN must be kept strictly confidential at all times.

3.3 SIGNMAN shall view any contravention of this Policy as very serious, and employees who are guilty of contravening the Policy will be subject to disciplinary action, which may result in summary dismissal.

4. STORAGE OF DOCUMENTS

Records of information will be stored for a reasonable period relevant to the purpose for which such information was provided by a disclosing party, or for such period as contractually may be applicable or as specifically determined by relevant legislation.

4.1 Electronic Storage

4.1.1 **The internal procedure in respect of electronic storage of information:** Important documents and information must be referred to and discussed with the information technology department of SIGNMAN who will arrange for the indexing, storage and retrieval thereof. This will be done in conjunction with the relevant departments concerned.

4.1.2 **Scanned documents:** If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to personnel. Any document containing information on the written particulars of an employee, including the employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years, must be retained for a period of 3 years after termination of employment.

5. TRANSBORDER INFORMATION FLOWS

5.1 SIGNMAN shall not transfer personal information of clients or employees to a third party situated in a foreign country unless:

5.1.1 The third party recipient of the information is subject to a law, binding corporate rules or binding contractual agreements which provide an adequate level of protection which effectively upholds principles for reasonable processing of such information which are substantially similar to the conditions for the lawful processing of personal information related to a natural person or juristic person in South Africa, and includes provisions which are substantially similar to the provisions of section 72 of POPI,

relating to the further transfer of personal information from the recipient to third parties situated in a foreign country;

5.1.2 Clients and employees consent to the transfer of information;

5.1.3 The transfer is necessary for the performance of a contract between a client or employee and SIGNMAN, or for the implementation and facilitation of pre-contractual measures;

5.1.4 The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the client or employee between SIGNMAN and a third party; and

5.1.5 The transfer is for the benefit of the client or employee, and it is not reasonably practicable to obtain the consent of the client or employee in respect of such transfer, and if it were reasonably practicable to obtain such consent, the client or employee would be likely to provide such consent.

6. DESTRUCTION OF DOCUMENTS

6.1 **Documents may be destroyed after the termination of the relevant retention periods. The compliance department will request departments to attend to the destruction of their documents and these requests shall be attended to as soon as possible.**

6.2 Each department is responsible for attending to the destruction of its documents, which must be performed on a regular basis. Files must be checked in order to ensure that they are to be destroyed, and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by SIGNMAN pending such return.

6.3 After completion of the process referred to in paragraph 6.2 above, the head of the department shall, in writing, authorise the removal and destruction of the documents in the authorisation document. These records will be retained by the compliance department.

6.4 The documents are then made available for collection by the contracted removers of SIGNMAN's documents, who also ensure that the documents are shredded before disposal. This also assists to ensure confidentiality of information.

6.5 Documents may also be stored off-site, in storage facilities approved by the Information Officer.

END