COMPLIANCE MANUAL

FOR THE IMPLEMENTATION OF THE

PROTECTION OF PERSONAL INFORMATION ACT 2013

CONTENT:

A. INTRODUCTION

The Protection of Personal Information Act POPI is intended to balance two competing interests - these are:

- Our individual constitutional rights to privacy (which requires our personal information to be protected) and
- The needs of our Society to have access to and to process (work with) our personal information for legitimate purposes, including the purpose of doing business.

This Compliance Manual sets out the framework for SODURBA CTO (hereafter referred to as "the CTO") compliance with POPI

Where reference is made to "processing" of personal information, this will include any activity in which information is worked with, from the time that information is collected, up to the time that the information is destroyed. Regardless of whether the information is worked with manually, or by automated system.

B. OUR UNDERTAKINGS TO OUR MEMBERS

1. We undertake 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 Members.

2. We undertake to process information only for the purpose for which it is intended, to enable us to do our work, as agreed with our Members.

3. Whenever necessary, we shall obtain Consent to process personal information.

4. Where we do not seek Consent, the processing of our Members' personal information will be following a legal obligation placed upon us, or to protect a legitimate interest that requires protection.

5. We shall stop processing personal information if the required Consentis withdrawn, or if a legitimate objection is raised.

6. We shall collect personal information directly from a Member whose information we require, unless:

   6.1 the information is of Public Record

   6.2 the Member Consents to the Collection of their personal from another source

6.3 the collection of the information from another source does not prejudice the Member

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

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

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

6.7 the information is required to maintain our legitimate interests, or

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

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

7. We shall advise our members of the purpose of the collection of the personal information

8. We shall retain records of the personal information we have collected for the minimum period as required by law unless the member has furnished their consent or instructed us to retain the records for a longer period.

9. We shall destroy or delete records of the personal information (so as to de-identify the member) as soon as reasonably possible after the time period for which we were entitled to hold the records have expired.

10. We shall restrict the processing of personal information:

    10.1 with accuracy of the information is contested, for a period sufficient to enable us to verify the accuracy of information, or

    10.2 with 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, or

    10.3 where the member requests that the personal information is not destroyed or deleted, but rather retained, or

    10.4 where the member requests that the personal information be transmitted to another automated data processing system.

11. The further processing of personal information shall only be undertaken:

    11.1 if the requirements of paragraphs 3, 6.1, 6.4, 6.5 or 6.6 above have been met;

    11.2 where the further processing is necessary because of a threat to public health or

public safety or to the life or health of a member, or a third party;

11.3 where the information is used for historical, statistical or research purposes and the identity of the member will not be disclosed, or

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

12. We undertake to ensure that the personal information which we collect and process is complete, accurate, not misleading and up to date.

13. We undertake to retain the physical file and electronic data related to the processing of the personal information.

14. We undertake to take special care with our member's bank details, and we are not entitled to obtain or disclose or procure the disclosure of such banking details unless we have the member's specific consent.

15. Any new members must be informed of their rights with regards the POPI Act and members must sign to acknowledge their understanding of their rights.

C. MEMBERS RIGHTS

1. In cases where the members consent is required to process their personal information, this consent may be withdrawn.

2. In cases where we process personal information without consent to protect a legitimate interest, to comply with the law or to pursue or protect our legitimate interests, the member has the right to object to such processing.

3. All members are entitled to lodge a complaint regarding our application of POPI with the Information Regulator.

4. A declaration must be obtained for the member's consent to process their personal information while we do our work for them, and less this consent has been obtained within another document signed by the member.

D. SECURITY SAFEGUARDS

1. In order to secure the integrity and confidentiality of the personal information in our possession, and to protect it against loss or damage or unauthorized access, we must continue to implement the following security safeguards:

1.1 The premises where records are kept must remain protected as far as reasonable.

1.2 Archived files must be stored again behind locked doors and access control to these storage facilities must be implemented.

1.3 All the user terminals are internal computer network, and our servers must be protected by passwords which must be changed on a regular basis.

1.4 Email infrastructure must comply with industry standard security safeguards and meet the General Data Protection Regulation (GDPR), which is standard in the European union.

1.5 Vulnerability assessments must be carried out on our digital infrastructure at least on an annual basis to identify weaknesses in our systems and to ensure we have adequate security in place.

1.6 We must use and ensure that all reasonable steps are taken to ensure computers and data storage is not compromised.

1.7 Our directors and staff must be trained to carry out their duties in compliance with POPI, and this training must be ongoing.

1.8 It must be a term of the contract with every director that they must maintain full confidentiality in respect of all our members' affairs, including our members' personal information.

1.9 Employment contracts for staff whose duty is to process the member's personal information, must include an obligation on the staff member (1) to maintain the Company's security measures, and (2) to notify their manager/supervisor immediately if there are reasonable grounds to believe that the personal information of a member has been accessed or acquired by any unauthorized person.

1.10 The processing of the personal information of our staff members must take place in accordance with the rules contained in the relevant labour legislation.

1.11 The digital work profiles and privileges of staff who have left our employee must be properly terminated.

1.12 The personal information of members and staff must be destroyed timeously in a manner that de-identifies the person.

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 or deficiencies.

E. SECURITY BREACHES

1. Should it appear that the personal information of a member has been accessed or acquired by an unauthorized person, we must notify the Information Regulator and the relevant member/s, unless we are no longer able to identify the member/s. This notification must take place as soon as reasonably possible.

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 member/s be delayed.

3. The notification to the member must be communicated in writing in one of the following ways, with a view to ensuring that the notification reads reaches the member:

   3.1 by mail to the member's last known physical or postal address

   3.2 by email to the member's last known email address

   3.3 by publication on our website or in the news media, or

   3.4 as directed by the Information Regulator.

4. This notification to the member must give sufficient information to enable the member to protect themselves against the potential consequences of the security breach, and must include:

   4.1 a description of the possible consequences of the breach,

   4.2 details of the measures that we intend to take or have taken to address the breach,

   4.3 the recommendation of what the member could do to mitigate the adverse effects of the breach, and

   4.4 if known, the identity of the person who may be may have accessed or acquired the personal information.

F. MEMBERS REQUESTING RECORDS

1. On production of proof of identity, any person is entitled to request that we confirm, free of charge, whether or not we hold any personal information about that person in our records.

2. If we hold such personal information, on request, and upon payment of a fee of **R150.00 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 of time, in a reasonable manner and in an understandable form.

3. A member 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. See form O. 4 below.

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

5. In all cases where the disclosure of a record will entail 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 shall

make their decision having regard to the provisions of Chapter 4 of Part 3 of the Promotion of Access to Information Act.

6. It's 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.

G. THE CORRECTION OF PERSONAL INFORMATION

1. A member is entitled to require as to correct or delete personal information that we have, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or which has been obtained unlawfully.

2. A member is also entitled to require us to destroy or delete records of personal information about the member that we are no longer authorized to retain.

3. Any such request must be made on the prescribed form, Form 4, referred to in section O below [Form 2 in the Regulations].

4. Upon receipt of such lawful request, we must comply as soon as reasonably practicable.

5. In the event that a dispute arises regarding the member's rights to have information corrected, and in the event that the member so requires, we must attach to information, in a way that it will always be read with information, an indication that the correction of the information has been requested but has not been made.

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

H. SPECIAL PERSONAL INFORMATION

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 behavior.

2. We should not process any of the Special Personal Information without the member’s consent, or where this is necessary for the establishment, exercise or defense of a right or an obligation in law.

3. Having regard to the nature of our work, it is unlikely that we will ever have to process special personal information but should it be necessary the guidance of the Information Officer, or their deputy/delegate, must be sought.

I. THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN

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

J. INFORMATION OFFICER

1. Our information officer is AMANDA JANSE VAN RENSBURG, her nomination was authorized by the CTO Chair and in writing. The authorization is on Form 9 referred to in section 'O' below. Our information Officer's responsibilities include:

   1.1 Ensuring compliance with POPI

   1.2 Dealing with requests received in Term of POPI

   1.3 Working with the Information Regulator in respect of investigations.

2. Our Information Officer must designate in writing, as many Deputy Information Officers, as are necessary, to perform the tasks mentioned in para.1 above. Such designation shall be done by completion of the prescribed form, a copy of which is in an Annexure to this Compliance Manual, see Form 8 referred to in section 'O' below.

3. Our Information Officer and our Deputy Information Officers must register themselves with the Information Regulator prior to taking up their duties, see Form 7 referred to in Section 'O' below.

4. In carrying out their duties, our Information Officers, must ensure that:

   4.1 the Compliance Manual is implemented

   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.

   4.3 That this Compliance Manual is developed, monitored maintained and made available.

   4.4 that internal measures are developed together with adequate systems to process requests for information or access to information.

   4.5 that internal awareness sessions are conducted regarding the provisions of POPI, the Regulations, Codes of Conduct or information obtained from the Information Regulator AND

   4.6 that copies of this manual or provided to persons at their request, hard copies to be provided upon payment of a fee (to be determined by the Information Regulator)

5. Guidance Notes on Information Officers have been published by the Information Regulator on 1st April 2021 and our Information and Deputy Information Officers must familiarize themselves with the contents thereof.

K. CIRCUMSTANCES REQUIRING PRIOR AUTHORIZATION

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

   1.1 In the event that we intend to utilise any unique identifiers of members (account numbers, file numbers or other numbers or codes allocated to members for the purpose of identifying them in our business) for any purpose other than original intention, or to link the information with information held by others.

   1.2 if we are processing information on criminal behavior or unlawful or objectionable conduct,

   1.3 if we are processing information for purposes of credit reporting (this will be important if we are making reports to assist with tenant profiling, for example, to TPN or ITC).

   1.4 if we are 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.

2. The Information Regulator must be notified of our attention to process any personal information as set out in paragraph 1.1 above 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 make a decision 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 Regulator does not make a decision within the stipulated time periods, we can assume that the decision is in our favor and commence processing the information.

L. DIRECT MARKETING

1. We may only carry out direct marketing (using any form of electronic communication) to members if:

   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

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

2. We may only approach members using their personal information, if we have obtained their personal information in the context of providing services associated with our estate agency business to them, and we may then only market estate agency services to them.

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.

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.

5. A request to receive direct marketing must be made in the prescribed manner and form.

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

M. TRANSBORDER INFORMATION FLOWS

1. We may not transfer members personal information to a third party in a foreign country, unless:

1.1 the member consents to this, or requests it, or

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 similar to POPI, and such third party is governed by similar rules which prohibit the onward transfer of the personal information to third party in another country, or

1.3 the transfer the personal information is required for the performance of the contract between ourselves and the member, or

1.4 the transfer is necessary for the conclusion or performance of a contract for the benefit of the member entered into between ourselves and the third party, or

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

N. OFFENSES AND PENALTIES

1. POPI provides for serious penalties for the contravention of its terms. For minor offenses 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.

2. Breaches of this Compliance Manual will also be viewed as a serious disciplinary offence.

3. It is therefore imperative that we comply strictly with the terms of this Compliance Manual and protect our member's personal information in the same way as if it was our own.

CONTACT DETAILS

You may contact us – Information Officer for Sodurba CTO

Attention: Amanda Janse van Rensburg

Telephone Number: 082 851 4787

Email: amanda@sodurba.co.za

30 June 2021