

FOXOLUTION SYSTEMS ENGINEERING (PTY) LTD

PRIVACY POLICY AND COMPLIANCE MANUAL FOR THE IMPLEMENTATION OF THE PROTECTION OF PERSONAL INFORMATION ACT OF 2013

CONTENTS:

| | | |
|----|--|---------|
| A. | Introduction | Page 2 |
| B. | Our Undertaking to our Clients | Page 2 |
| C. | Our Client's Rights | Page 4 |
| D. | Security Safeguards | Page 4 |
| E. | Security Breaches | Page 6 |
| F. | Clients Requesting Records | Page 7 |
| G. | The Correction of Personal Information | Page 8 |
| H. | Special Personal Information | Page 8 |
| I. | Processing of Personal Information of Children | Page 8 |
| J. | Information Officer | Page 9 |
| K. | Circumstances Requiring Prior Authorization | Page 9 |
| L. | Direct Marketing | Page 10 |
| M. | Transborder Information Flows | Page 11 |
| N. | Offences and Penalties | Page 11 |
| O. | Schedule of Annexures and Forms | Page 11 |

A. INTRODUCTION

The Protection of Personal Information Act (POPIA) is intended to balance 2 competing interests. These are:

1. Our individual constitutional rights to privacy (which requires our personal information to be protected); and
2. 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 our company's compliance with POPIA.

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

B. OUR UNDERTAKINGS TO OUR CLIENTS:

1. We undertake to follow POPIA at all relevant times and to process personal information lawfully and reasonably, so as not to infringe unnecessarily on the privacy of our clients.
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 clients.
3. Whenever necessary, we shall obtain consent to process personal information.
4. Where we do not seek consent, the processing of our client's 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 We shall stop processing personal information if the required consent is withdrawn, or if a legitimate objection is raised.
6. We shall collect personal information directly from the client whose information we require, unless:
 - 6.1 the information is of public record, or
 - 6.2 the client has consented to the collection of their personal information from another source, or
 - 6.3 the collection of the information from another source does not prejudice the client, or
 - 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 any relevant Act (e.g. Gas Act, Environmental Acts, OHSA etc.)
 - 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 clients 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 client 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 client) 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 where the accuracy of the information is contested, for a period sufficient to enable us to verify the accuracy of the information;
 - 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;
 - 10.3 where the client requests that the personal information is not destroyed or deleted, but rather retained; or
 - 10.4 where the client 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 the client, or a third person;
 - 11.3 where the information is used for historical, statistical or research purposes and the identity of the client will not be disclosed; or
 - 11.4 where this is required by the Information Regulator appointed in terms of POPIA.

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 the electronic data related to the processing of the personal information.
14. We undertake to take special care with our client's bank account details, and we are not entitled to obtain or disclose or procure the disclosure of such banking details unless we have the client's specific consent.
15. **Annexure A** letter shall be sent to every client when we commence an agreement of any sort, to advise them of our duty to them in terms of POPIA.

C. OUR CLIENT'S RIGHTS

1. In cases where the client's 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 client has the right to object to such processing.
3. All clients are entitled to lodge a complaint regarding our application of POPIA with the Information Regulator.
4. Consent shall be obtained from and signed by clients (**See Form 1**) when we commence in providing a service of any sort, or as provided for within a relevant agreement or application, in order to process their personal information while we do our work for them.

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 unauthorised access, we must continue to implement the following security safeguards as identified by our PIIA (Personal Information Impact Assessment) and Data Audit, as well as our GAP Risk Analysis:
 - 1.1 Our various business premises where records are kept must remain protected by access control measures, locked, alarmed and secured accordingly. Physical files and documents must not be visible to anyone other than the personnel authorised to work with them.
 - 1.2 Archived files must be stored behind locked doors and restricted access control measures to these storage areas must be implemented.
 - 1.3 All the user terminals on our internal computer networks, devices, systems and any employee independent devices, cell phones, and computers must be protected by passwords which must be changed on a regular basis. Computers and devices must be switched off and shut down when not in

use. Employees must log out of all software, programs and other online applications when not in use.

- 1.4 We will maintain a “Clean Desk” and “Clear Screen” policy.
- 1.5 Our email infrastructure must comply with industry standard security safeguards with the necessary antivirus protection and encrypted web based storage.
- 1.6 Our website and server infrastructure must comply with the industry standard security safeguards and meet the GDPR, through third party service providers and their compliance procedures.
- 1.7 Any security cameras we may use are for security purposes only and any recordings will only be accessible by the relevant security personnel or authorised employee. DVR equipment will remain secure and protected in a locked location. Footage will not be utilised for any means other than what might be required in terms of a legal proceeding related to a security breach. Once footage is no longer required it will be permanently deleted.
- 1.8 Any third party programs and software we use, must comply with the industry relevant security safeguards with adequate protections and data encryptions in place.
- 1.9 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.
- 1.10 We must use an internationally recognised Firewall to protect the data on our local servers, and we must run antivirus scans at least every day to ensure our systems are kept updated with the latest patches. The security of this system must comply with the GDPR of the European Union.
- 1.11 Our staff must be trained to carry out their duties in compliance with POPIA, and this training must be ongoing.
- 1.12 It must be a term of the contract with every staff member that they must maintain full confidentiality in respect of all of our clients’ affairs, including our clients’ personal information.
- 1.13 Employment contracts for staff whose duty it is to process a client’s personal information, must include an obligation on the staff member (1) to maintain the Company’s security measures, and (2) to notify the Information Officer immediately if there are reasonable grounds to believe that the personal information of a client has been accessed or acquired by any unauthorised person.
- 1.14 The processing of the personal information of our staff members must take place in accordance with the rules contained in the relevant labour legislation.

- 1.15 The digital work profiles and privileges of staff who have left our employ must be properly terminated.
- 1.16 The personal information of clients and staff must be destroyed timeously in a manner that de-identifies the person, when the prescribed period identified per the relevant legal requirement has passed. This includes, but is not limited to the following:
 - 1.17 For information that may be required in terms of SARS (South African Revenue Service) and FIC (Financial Intelligence Centre) regulations, the retention period is 5 (five) years.
 - 1.18 For information that may be required in terms of Auditing, the retention period is 5 (five years).
 - 1.19 For information that may be required in terms of the CPA (Consumer Protection Act) the retention period is 3 (three) years.
 - 1.20 For information that may be required in terms of the Electronic Communication and Transaction Act retention period is at least 1 (one) years after the information is no longer used.
 - 1.21 For information collected in terms of the Basic Conditions of Employment Act, the retention period is 3 (three) years from the date of the last entry recorded.
 - 1.22 In terms of the Labour Relations Act, the retention period that applies to personal information related to sections 53 (4) and 98 (4) is 3 (three) years and if Schedule 8 Section 5 applies, then retention of data is indefinite.
 - 1.23 For information required in terms of the Unemployment Insurance Act, Tax Administration Act and Income Tax Act, retention of data is 5 (five) years.
 - 1.24 Please refer to the SAICA Retention of Records Guide, included as **Annexure B**, for a more comprehensive list.
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 client has been accessed or acquired by an unauthorised person, we must notify the Information Regulator and the relevant client/s, unless we are no longer able to identify the client/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 client/s be delayed.

3. The notification to the client must be communicated in writing in one of the following ways, with a view to ensuring that the notification reaches the client:
 - 3.1 by mail to the client's last known physical or postal address;
 - 3.2 by email to the client's last known email address;
 - 3.3 by publication on a relevant public platform, still maintaining the integrity of the client; or
 - 3.4 as directed by the Information Regulator.
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:
 - 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 client could do to mitigate the adverse effects of the breach; and
 - 4.4 if known, the identity of the person who may have accessed, or acquired the personal information.

F. CLIENTS 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 R500.00, 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 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. **(See Form 2)**
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.
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 shall make their decision having regard to the

provisions of Chapter 4 of Part 3 of the Promotion of Access to Information Act (PAIA).

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.

G. THE CORRECTION OF PERSONAL INFORMATION

1. A client is entitled to require us 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 client is also entitled to require us to destroy or delete records of personal information about the client that we are no longer authorised to retain.
3. Any such request must be made on the prescribed form. **(See Form 3)**
4. Upon receipt of such a lawful request, we must comply as soon as reasonably practicable.
5. In the event that a dispute arises regarding the client's rights to have information corrected, and in the event that 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.
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 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 behaviour.
2. We shall not process any of this Special Personal Information without the client's consent, or where this is necessary for the establishment, exercise or defense of a right or an obligation in law.
3. Regarding the nature of our work, it is unlikely that we will ever have to process this special personal information, but should it be necessary the guidance of the Information Officer, or their deputy/delegate, must be sought in consultation with the Information Regulator.

I. THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN

1. The nature of our work does not require us to process the personal information of a child.

J. INFORMATION OFFICER

1. Our Information Officer is Craig Motherwell. Our Information Officer's responsibilities include:
 - 1.1 Ensuring compliance with POPIA.
 - 1.2 Dealing with requests which we receive in terms of POPIA.
 - 1.3 Working with the Information Regulator in relation to investigations.
2. Our Information Officer can designate in writing as many Deputy Information Officers as are necessary to perform the tasks mentioned in paragraph 1 above.
3. Our Information Officer and our Deputy Information Officers, if applicable, must register themselves with the Information Regulator prior to taking up their duties.
4. In carrying out their duties, our Information Officer must ensure that:
 - 4.1 this Compliance Manual containing the Privacy Policy, Forms and other applicable documentation 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 and Privacy Policy 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 POPIA, the Regulations, codes of conduct or information obtained from the Information Regulator; and
 - 4.6 that copies of this manual are 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 1 April 2021) and our Information Officer and any deputy Information Officers must familiarize themselves with the content of these notes.

K. CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION

1. In the following circumstances, we will require prior authorisation from the Information Regulator before processing any personal information:
 - 1.1 In the event that we intend to utilise any unique identifiers of clients (account numbers, file numbers or other numbers or codes allocated to clients for the purposes of identifying them in our business) for any purpose other than the original intention, or to link the information with information held by others;

- 1.2 if we are processing information on criminal behaviour or unlawful or objectionable conduct;
 - 1.3 if we are processing information for the purposes of credit reporting;
 - 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 intention 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 favour and commence processing the information.

Section 57 (3) and Section 58 of the Act is not applicable if a code of conduct has been issued and has come into force in terms of Chapter 7 of the Act in a specific sector or sectors of society, as has been done by the Credit Bureau Association on the 14th April 2021 regarding 1.3 above.

L. DIRECT MARKETING

1. We may only carry out direct marketing (using any form of electronic communication) to clients 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 clients using their personal information, if we have obtained their personal information in the context of providing services associated with our real estate business to them, and we may then only market such property related 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 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, **See Form 4**.
6. All direct marketing communications must disclose our identity and contain an address or other contact details to which the client may send a request that the communications cease.

M. TRANSBORDER INFORMATION FLOWS

1. We may not transfer a client's personal information to a third party in a foreign country, unless:
 - 1.1 the client 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 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
 - 1.3 the transfer of the personal information is required for the performance of the contract between ourselves and the client; or
 - 1.4 the transfer is necessary for the conclusion or performance of a contract for the benefit of the client entered into between ourselves and the third party; or
 - 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.

N. OFFENCES AND PENALTIES

1. POPIA provides for serious penalties for the contravention of its terms.
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 client's personal information in the same way as if it was our own.

O. SCHEDULE OF ANNEXURES AND FORMS

| | |
|-------------|---|
| Annexure A: | Letter to client. |
| Annexure B: | Retention Of Records Guide by SAICA. |
| Form 1: | Client's consent to process personal information. |
| Form 2: | Objection to the Processing of Personal Information. |
| Form 3: | Request for correction or deletion of personal information. |
| Form 4: | Application for consent to direct marketing. |