TECHNOLUTIONS PTY LTD

2011/011660/07

19 KENDAL ROAD, DIEP RIVER, CAPE TOWN, 8001

Email: hello@o-it.co.za

COMPLIANCE MANUAL

FOR THE IMPLEMENTATION OF THE

PROTECTION OF PERSONAL INFORMATION ACT OF 2013

DATE FIRST COMPILED: 15 June 2021

DATE REVISED: 25 June 2021

VERSION NUMBER: 1.3

CONTENTS:

A. INTRODUCTION

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

1. The individual's constitutional rights to privacy (and subsequent protection of personal information); and
2. The needs of our society, and economy, to have access to and to process personal information for legitimate business/ legal purposes.

This Compliance Manual sets out the framework for our company's compliance with POPI, as well as the Promotion of Access to Information Act (PAIA).

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 DATA PRIVACY UNDERTAKINGS:

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 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 by law, 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 We shall stop processing personal information if the required consent is withdrawn, or if a legitimate objection is raised.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

6.6 the information collected is required for the conduct of proceedings in any court or tribunal, 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 undertake to 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 that information) as soon as reasonably possible after the time period for which the records had to be held has 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 the processing is required by the Information Regulator (South Africa).

12. We will take all reasonable measures to ensure that the personal information which we collect and process is complete, accurate and up to date.

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 written consent.

C. OUR CLIENT'S RIGHTS

1. In cases where the client's consent is required to process their personal information, the client is entitled to withdraw their consent.

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 the POPI Act with the Information Regulator.

THE INFORMATION REGULATOR (SOUTH AFRICA)

Email: complaints.IR@justice.gov.za

Physical address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001

D. SECURITY SAFEGUARDS

[The clauses below, especially clauses 1.3 to 1.6, contain suggested measures only and must be edited and adjusted, depending on the levels of security that each entity believes is reasonable and appropriate to their business and sufficient to meet the requirements of POPI. You will need the assistance of at least your IT administrator/service provider/consultant to assist with the security of your IT infrastructure.]

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

   1.1 Our business premises where records are kept must remain protected by access control, burglar alarms and armed response.

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

   1.3 All the users, mobile devices, machines on our LAN, (Local Area Network), and our servers must be protected by passwords which must be changed on a regular basis.

   1.4 Our email infrastructure and Office 365 complies with industry standard security safeguards. We utilize Multi Factor Authentication.

   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 International Standard Firewalls to protect the data on our hosted servers, and we run antivirus protection at least once a day to ensure our systems are kept updated with the latest patches.

1.7 Our systems are protected with VPN Access, (Virtual Private Network), and the information is only accessible as per this protocol or direct access from our office.

1.8 Any information that we host for a client in a backup format is encrypted.

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

1.10 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.

1.11 Employment contracts for staff whose duty it is to process a client's personal information, includes an obligation on the staff member (1) to maintain the Company's security measures, and (2) to notify their manager/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.

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

1.13 The digital access of staff who have left our employ must be properly terminated as soon as possible and their data archived.

1.14 The personal information of clients 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. If it appears that there is a data privacy breach, where the personal information we store has been accessed or acquired unlawfully, 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 our website or in the news media; 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 the personal information.

F. CLIENTS REQUESTING RECORDS

1. On production of certified (not older than 6 months) proof of identity, any person is entitled to request confirmation, free of charge, of 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 R250-00, 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. The request for the record must be completed on the prescribed form for "Request for Access to Record of Private Body" and submitted to hello@o-it.co.za. This is attached below as an annexure.

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 must be made on the prescribed application form.

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. The client will be informed accordingly.

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.

6. If a request for personal information is made and part of the requested information may, or must be refused, every other part will 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, attached hereunder as an annexure.

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

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 anyone accessing 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 we have decided and 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 such processing is necessary for the establishment, exercise or defense of a right or an obligation in law.

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. OUR INFORMATION OFFICER

1. Our Information Officer is Pieter Paul Kotze who is our Managing Director or someone in a senior management position nominated and authorised in writing. Our Information Officer's responsibilities include:

   1.1 Ensuring compliance with POPI.

   1.2 Dealing with requests which we receive in terms of POPI.

   1.3 Working with the Information Regulator in relation to investigations.

2. In carrying out their duties, our Information Officer must ensure that:

   2.1 this Compliance Manual is implemented;

   2.2 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;

   2.3 that this Compliance Manual is developed, monitored, maintained and made available;

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

   2.5 that internal awareness sessions are conducted regarding the provisions of POPI, the Regulations, codes of conduct or information obtained from the Information Regulator; and

   2.6 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).

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.

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 business to them, and we may then only market those related business services to them.

3. We may only carry out direct marketing (using any form of electronic communication) to non-clients 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.

5. A request for consent to receive direct marketing must be made in the prescribed manner and form. The prescribed form that we must use is attached to this manual.

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 POPI, 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. TYPES OF RECORDS HELD

1. Companies Act Records
   - Company Incorporation
   - Names of Directors
2. Financial Records
   - Financial Statements
   - Accounting Records
   - Financial Agreements
3. Agreements or Contract Records
   - Standard Agreements
   - Contracts concluded with Companies
   - Contracts concluded with Customers
   - Third Party Contracts (such as Service Level Agreements etc.)
   - Suppliers Contracts
4. Employees
   - List of Employees
5. Company Policies and Directives
   - Internal IT Policies relating to employees and the company
7. Customer Information
   - Customer Details
   - Contact details of individuals within Customers
   - Communications with Customers
8. Systems, Solutions, and Information Technology
   - Intellectual property pertaining to solutions and products developed.
   - Usage of solutions and products

O. SCHEDULE OF ANNEXURES AND FORMS

1. Form 1: Request for Access to Record of Private Body
2. Form 2: Request for Correction or Deletion of Personal Information
3. Form 3: Objection to the Processing of Personal Information
4. Form 4: Application for consent to direct marketing (Form 4 of the Regulations)