vitallegal

Because every case is vital

lifesaver

to your rescue

Protection of **Personal Information Act** (POPIA)

INFORMATION REGULATOR

PROTECTION OF PERSONAL INFORMATION ACT 2013 (ACT NO. 4 OF 2013)
REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION

The Information Regulator has, under section 112(2) of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013), made the regulations in the schedule.

VITAL LEGAL SERVICES PTY LTD FSP40817

Reg. No. 2013/150097/07 | Vital Legal Services (Pty) Ltd is an authorised Financial Services Provider, FSP No. 40817
Vital Legal Services (Pty) Ltd products are underwritten by GuardRisk Insurance Company, a licensed non-life insurer and authorised Financial Services Provider, FSP No. 75

GUARDRISK TAILORED RISK SOLUTIONS
AUTHORISED FSP (75) AND A LICENSED NON-LIFE INSURER. AUTHORISED FSP 40817

AZOZA

1. INTRODUCTION

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA").

POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

Through the provision of quality services, the organisation is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.

A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

Given the importance of privacy, the organisation is committed to effectively managing personal information in accordance with POPIA's provisions.

2. DEFINITIONS

In these Regulations, any word or expression to which a meaning has been assigned in the Act has the meaning so assigned and, unless the context otherwise indicates:

Personal Information

Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to, information concerning:

- Race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;
- Information relating to the education or the medical, financial, criminal or employment history of the person;
- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- The biometric information of the person;
- The personal opinions, views or preferences of the person;
- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature, or further correspondence that would reveal the contents of the original correspondence;
- The views or opinions of another individual about the person;
- 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.

Data Subject

This refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies the organisation with products or services.

Data Message

Includes a data message as defined in section 1 of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002).

Responsible Parties

The responsible parties are the entities that need the personal information for a particular reason and determine the purpose of and means for processing the personal information. In this case, the organisation or other third party to which the data belongs is the responsible party.

Operator

An operator means a person or entity who processes personal information for responsible parties in terms of a contract or mandate, without coming under the direct authority of that party, such as a third-party service provider that has contracted with the organisation to shred documents containing personal information.

Information Officer/ Deputy Information Officer

The Information Officer and Deputy Information Officer are responsible for ensuring the organisation's compliance with POPIA.

Where no Information Officer is appointed, the head of the organisation will be responsible for performing the Information Officer's duties with the assistance of identified Deputy Information Officers.

Processing

The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

- The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- Dissemination by means of transmission, distribution or making available in any other Form; or
- Merging, linking, as well as any restriction, degradation, erasure or destruction of information.

Record

Means any recorded information, regardless of Form or medium, including:

- Writing on any material;
- Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph or drawing;
- Photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced.

Filing System

Means any structured set of personal information, whether centralised, decentralised or dispersed on a Functional or geographical basis, which is accessible according to specific criteria.

Unique Identifier

Means any identifier that is assigned to a data subject and is used by the Responsible Parties for the purposes of the operations of those Responsible Parties and that uniquely identifies that data subject in relation to those Responsible Parties.

De-Identify

In relation to personal information of a data subject, it means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

Re-Identify

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

Consent

Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

Direct Marketing

Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- Promoting or offering to supply, in the ordinary course of business, any products or services to the data subject; or
- Requesting the data subject to make a donation of any kind for any reason.

Biometrics

Means a technique of personal identification that is based on physical, physiological or behavioural characterisation, including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

Form(s)

Form(s) as referred to in these Regulations means a form referred to in the annexures to these Regulations or any form which is substantially similar to that form.

Signature

Signature includes an electronic signature as defined in section 1 of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002).

Submit

Submit means submit by -

- Data message
- Electronic Communication
- Registered Post
- Electronic Mail
- Personal Delivery

The Act

Means the Protection of Personal Information Act, 2013 (Act No. 4 of 2013).

Writing

Includes writing as referred to in section 12 of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002).

3. POLICY PURPOSE

The purpose of this policy is to protect the organisation from the compliance risks associated with the protection of personal information, which includes:

- Breaches of confidentiality. For instance, the organisation could suffer a loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose the organisation uses information relating to them.
- Reputational damage. For instance, the organisation could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by the organisation.

This policy demonstrates the organisation's commitment to protecting the privacy rights of data subjects in the following manner:

- Through formalising desired behaviour and directing compliance with the provisions of POPIA and best practice.
- By cultivating an organisational culture that recognises privacy as a valuable human right.
- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
- By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the organisation.
- By assigning specific duties and responsibilities to the Information Officer, including the appointment of Deputy Information Officer/s where necessary, in order to protect the interests of the organisation and data subjects.
- By raising awareness through training and providing guidance to individuals who process personal information, they can act confidently and consistently.

4. POLICY APPLICATION

This policy and its guiding principles apply to:

- The organisation's governing body
- All branches, business units and divisions of the organisation
- All employees
- All contractors, suppliers and other persons acting on behalf of the organisation

The policy's guiding principles find application in all situations and must be read in conjunction with the organisation's PAIA Policy as required by the Promotion of Access to Information Act.

The legal duty to comply with POPIA's provisions is activated in any situation where there is:

- A processing of personal information
- Entered into a record
- By or for a Responsible Person
- Who is domiciled in South Africa.

POPIA does not apply in situations where the processing of personal information:

- Is concluded in the course of purely personal or household activities, or
- Where the personal information has been de-identified.

5. OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION

1. A data subject who wishes to object to the processing of personal information in terms of section 11 (3)(a) of the Act must submit the objection to the responsible party on Form 1 (available on request).
2. The responsible party, or a designated person, must render such reasonable assistance as is necessary, free of charge, to enable the data subject to make an objection on Form 1 (available on request).

6. RIGHTS OF DATA SUBJECTS

Where appropriate, the organisation will ensure that its clients and customers are made aware of their rights as data subjects.

The organisation will ensure that it gives effect to the following six rights.

6.1. The Right to Access Personal Information

The organisation recognises that a data subject has the right to establish whether the organisation holds personal information related to him, her or it, including the right to request access to that personal information.

6.2. The Right to have Personal Information Corrected or Deleted

The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where the organisation is no longer authorised to retain the personal information, where that information is not required to be held in terms of relevant Law.

6.3. The Right to Object to the Processing of Personal Information

The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information.

In such circumstances, the organisation will give due consideration to the request and the requirements of POPIA. The organisation may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record-keeping requirements, also approve the destruction of the personal information.

6.4. The Right to Object to Direct Marketing

The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

6.5. The Right to Complain to the Information Regulator

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

6.6. The Right to be Informed

The data subject has the right to be notified that his, her, or its personal information is being collected by the organisation.

The data subject also has the right to be notified in any situation where the organisation has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

7. REQUEST FOR DATA SUBJECT'S CONSENT TO PROCESS PERSONAL INFORMATION

A responsible party who wishes to process personal information of a data subject for direct marketing by electronic communication must, in terms of section 69(2) of the Act, submit a request for written consent to that data subject on Form 4 (available on request).

8. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURES

Data subjects have the right to:

- Request what personal information the organisation holds about them and why,
- Request access to their personal information,
- Request the destruction or deletion of their personal information (on reasonable grounds and
- Be informed on how to keep their personal information up to date.

Access to information requests can be made by email, addressed to the Information Officer or Deputy Information Officer. The Information Officer or Deputy Information Officer will provide the data subject with a "Personal Information Request Form".

Once the completed Form has been received, the Deputy Information Officer will verify the identity of the data subject prior to handing over any personal information. All access requests will be processed and considered against the organisation's PAIA Policy.

The Deputy Information Officer will process all requests within a reasonable time.

9. REQUEST FOR CORRECTION, DELETION OF PERSONAL INFORMATION OR DESTRUCTION AND OR DELETION OF RECORDS OF PERSONAL INFORMATION

1. A data subject who wishes to request a correction or deletion of personal information or the destruction or deletion of a record of personal information in terms of section 24(1) of the Act must submit a request to the responsible party on Form 2. (Available on request)

2. The responsible party, or a designated person, must render such reasonable assistance, as is necessary, free of charge, to enable a data subject to complete Form 2. (Available on request)

10. INFORMATION OFFICER OR DEPUTY INFORMATION OFFICER

The organisation's Information Officer or Deputy Information Officer is responsible for ensuring compliance with POPIA.

1. An information officer or Deputy Information Officer must, in addition to the responsibilities referred to in section 55(1) of the Act, ensure that -

    a. Compliance Framework is developed, implemented, monitored and maintained;
    b. 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.
    c. A manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)
    d. Internal measures are developed together with adequate systems to process requests for information or access thereto; and
    e. Internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.

2. The information officer or Deputy Information Officer shall, upon request by any person, provide copies of the manual to that person.

11. SPECIFIC DUTIES & RESPONSIBILITIES

Governing Body

The organisation's governing body cannot delegate its accountability and is ultimately answerable for ensuring that the organisation meets its legal obligations in terms of POPIA.

The governing body may, however, delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The governing body is responsible for ensuring that:

All persons responsible for the processing of personal information on behalf of the organisation:

- Are appropriately trained and supervised to do so
- Understand that they are contractually obligated to protect the personal information they come into contact with, and
- Are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.

Data subjects who want to enquire about their personal information are made aware of the procedure that needs to be followed should they wish to do so.

The scheduling of periodic POPI audits in order to accurately assess and review the ways in which the organisation collects, holds, uses, shares, discloses, destroys and processes personal information.

Retention of Data

All personal information in the possession of the organisation must be stored, retained and destroyed in accordance with the legislation applicable to the specific information. Personal information shall not be retained longer than required to fulfil the purpose for the processing or longer than required by applicable legislation. Once the purpose for processing or the retention period provided under applicable legislation expires, the Personal Information must be destroyed and/or deleted, unless retained for statistical, historical or research purposes.

Information Officer/ Deputy Information Officer

The organisation's Information Officer and Deputy Information Officer/s are responsible for:

- Taking steps to ensure the organisation's reasonable compliance with the provisions of POPIA.
- Keeping the governing body updated about the organisation's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer or Deputy Information Officer/s must inform and advise the governing body, and the business of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with the organisation's personal information processing procedures. This will include reviewing the organisation's information protection procedures and related policies.
- Ensuring that POPI audits are scheduled and conducted on at least an annual basis.
- Ensuring that the organisation makes it convenient for data subjects who want to update their personal information or submit POPI-related complaints to the organisation.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about the organisation's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the organisation.

- Addressing employees' POPIA-related questions.
- Addressing all POPIA-related requests and complaints made by the organisation's data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officer and Deputy Information Officer will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

The Deputy Information Officer/swill assist the Information Officer in performing his or her duties.

IT Department

The organisation's IT Department is responsible for:

- Ensuring that the organisation's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- Ensuring that all electronically held personal information is kept only on designated drives and servers.
- Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- Ensuring that all electronically stored personal information is backed up and tested on a regular basis.
- Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Ensuring that personal information being transferred electronically is encrypted.
- Ensuring that a firewall and the latest security software protect all servers and computers containing personal information.
- Performing regular IT audits to ensure that the security of the organisation's hardware and software systems is functioning properly.
- Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
- If applicable, performing a proper due diligence review before contracting with operators or any other third-party service providers to process personal information on the organisation's behalf. For instance, cloud computing services.

Employees and other Persons acting on behalf of the Organisation

Employees and other persons acting on behalf of the organisation will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

Employees and other persons acting on behalf of the organisation are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of the organisation may not directly or indirectly utilise, disclose or make public in any manner to any person or third party, either within the organisation or externally, any personal information, unless such information is already publicly known or the disclosure is necessary for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of the organisation must request assistance from their line manager or the Deputy Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of the organisation will only process personal information where:

- The data subject, or a competent person where the data subject is a child, consents to the processing; or
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- The processing complies with an obligation imposed by law on the Responsible Parties; or
- The processing protects a legitimate interest of the data subject; or
- The processing is necessary for pursuing the legitimate interests of the organisation or of a third party to whom the information is supplied. Furthermore, personal information will only be processed where the data subject:
    - Clearly understands why and for what purpose his, her, or its personal information is being collected; and
    - Has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information..

Employees and other persons acting on behalf of the organisation will, consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

Consent can be obtained in written form, which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the organisation will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- The personal information has been made public, or
- Where valid consent has been given to a third party, or
- The information is necessary for effe.

Employees and other persons acting on behalf of the organisation will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smartphones. All personal information must be accessed and updated from the organisation's central database or a dedicated server.

- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this must be requested from the relevant line manager, who must obtain approval from both the Information Officer and Deputy Information Officer.
- Transfer personal information outside of South Africa without the express permission of the Deputy Information Officer and the Information Officer.

Employees and other persons acting on behalf of the organisation are responsible for:

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- Ensuring that personal information is encrypted before sending or sharing the information electronically or sharing via secure FTP sites. The IT department will assist employees and, where required, other persons acting on behalf of the organisation, with the sending or sharing of personal information to or with authorised external persons.
- Ensuring that all computers, laptops and devices such as tablets, flash drives, and smartphones that store personal information are password-protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- Ensuring that where personal information is stored on removable storage media such as external drives, CDs or DVDs, these are kept locked away securely when not being used.
- Ensuring that where personal information is stored on paper, such hard copy records are kept in a secure place where unauthorised people cannot access it, such as in a locked drawer of a filing cabinet.
- Ensuring that where personal information has been printed out, the paper printouts are not left unattended where unauthorised individuals could see or copy them, such as close to the printer.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Deputy Information Officer to delete or dispose of the personal information appropriately.
- Undergo POPI Awareness training from time to time.
- Where an employee, or a person acting on behalf of the organisation, becomes aware or suspicious of any security breach, such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or Deputy Information Officer..

12. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of the organisation will at all times be subject to, and act in accordance with, the following guiding principles:

Accountability

Failing to comply with POPIA could potentially damage the organisation's reputation or expose the organisation to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

The organisation will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, the organisation will take appropriate sanctions, which may include disciplinary action, against those individuals who, through their intentional or negligent actions and/or omissions, fail to comply with the principles and responsibilities outlined in this policy.

Processing Limitation

The organisation will ensure that personal information under its control is processed:

- In a fair, lawful and non-excessive manner, and
- Only with the informed consent of the data subject, and
- Only for a specifically defined purpose.

The organisation will inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent before processing personal information. This consent may be given in the Form of an application Form completed by the individual.

Alternatively, where services or transactions are concluded over the telephone, the organisation will maintain a voice recording of the stated purpose for collecting the personal information, followed by the data subject's subsequent consent.

The organisation will under no circumstances distribute or share personal information between separate legal entities, associated organisations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the organisation's business and be provided with the reasons for doing so.

Purpose Specification

All of the organisation's business units and operations must be informed by the principle of transparency. The organisation will process personal information only for specific, explicitly defined and legitimate reasons. The organisation will inform data subjects of these reasons before collecting or recording the data subject's personal information.

Further Processing Limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

Therefore, where the organisation seeks to process personal information it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, the organisation will first obtain additional consent from the data subject.

Information Quality

The organisation will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

The more important it is that the personal information is accurate, the greater the effort the organisation will put into ensuring its accuracy.

Where personal information is collected or received from third parties, the organisation will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources or other means.

Open Communication

The organisation will take reasonable steps to ensure that data subjects are notified (are at all times aware) that their personal information is being collected, including the purpose for which it is being collected and processed.

The organisation will ensure that it maintains contractability via its website or call centre for data subjects who want to:

- Enquire whether the organisation holds related personal information, or
- Request access to related personal information, or
- Request the organisation to update or correct related personal information, or
- Make a complaint concerning the processing of personal information.

Security Safeguards

The organisation will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

Security measures will also be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit records, the greater the security required.

The organisation will continuously review its security controls, which will include regular testing of protocols and measures put in place to combat cyber-attacks on the organisation's IT network.

The organisation will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

The organisation will ensure that, where the retention of data requirement in terms of the applicable law has expired, data back-ups are taken offline, and made inaccessible and where necessary, personal information is scrubbed from a record within the database.

The organisation's code of conduct handbook codifies what is deemed acceptable conduct for employees performing their work as it relates to confidentiality and the security of personal information of customers, suppliers, and the organisation. It prohibits any Form of misconduct in relation to the unauthorised access, use, disclosure and dissemination of personal information. All new and current employees are expected to familiarise themselves with and adhere to the policies of the organisation, with formalised consequences for non-compliance that could lead to disciplinary action, including dismissal.

The organisation's operators and third-party service providers will be required to enter into service level agreements with the organisation where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

Data Subject Participation

A data subject may request the correction or deletion of his, her or its personal information held by the organisation.

The organisation will ensure that it provides a Facility For data subjects who want to request the correction or deletion of their personal information.

Deletion of data will be subject to data retention requirements in terms of the applicable Law.

Where applicable, the organisation will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

13. CROSS BORDER SHARING

Personal information transferred to third parties or even stored on cloud servers in jurisdictions outside SA may only do so under these conditions:

- The data subject must consent to the cross-border transmission/storage,
- Transfer or storage can only occur if the data protection laws governing that jurisdiction, corporate policies of the third party provider or agreement/mandate prescribing conditions for processing personal information are similar to POPI, or
- The transfer must be necessary for the performance of a contract or be for the benefit of the data subject and;
- An agreement or mandate must be in place with the third party or provider to protect our POPI interest, after evaluating the adequacy of the security measures to determine the appropriate protection of the personal information.

14. DIRECT MARKETING

Direct Marketing by means of Unsolicited Electronic Communications

The processing of personal information of a data subject for direct marketing by means of any Form of electronic communication, including automatic calling machines, Facsimile machines, SMSs or e-mail.

Conditions For Direct marketing, via electronic means, without requiring explicit consent first (only applicable to your existing clients- not prospective clients):

- You obtained the contact details of the data subject in the context of the sale of a product or service,
- You are marketing your own similar products or services to your client and
- You gave your customer a reasonable opportunity to object, Free of charge and in a manner Free of unnecessary formalities, to the use of his, her or its electronic details for marketing-
  - At the time when the information was collected, and
  - On the occasion of each communication with your customer, for marketing, if the data subject has not initially refused such use.

If all three conditions have not been met, you MUST obtain explicit consent before using the data subject's personal information for Direct marketing via any electronic means.

The Responsible party may approach a data subject whose consent is required (and who has not previously withheld such consent), ONLY ONCE, to request the consent of that data subject.

Any communication for direct marketing must contain details of the identity of the sender or the person on whose behalf the communication has been sent, including an opt-out option or contact details to which the recipient may send a request that such communications cease.

Direct Marketing Conducted in Person, by Mail or Telephonically

Direct marketing conducted in person, by mail, or telephonically (like in a call centre environment) does not require explicit consent before marketing. The data subject may, however, object at any time to the processing of personal information for direct marketing.

15. INCIDENT MANAGEMENT

A privacy incident is the loss of control, compromise, unauthorised disclosure, unauthorised acquisition, unauthorised access, or any similar term referring to situations where persons other than authorised users and for other than an authorised purpose have access or potential access to personal information or special personal information.

Once a privacy incident becomes known or has been identified either by staff, customers or reported by suppliers, partners or Operators, the Deputy Information Officer or Information Officer must be immediately notified. Any immediate action to mitigate further risk must be prioritised. An investigation into the cause, extent and severity of the incident will be investigated by the Deputy Information Officer.

The Deputy Information Officer will log the incident report on Centricity within 2 days of the incident. Corrective action and target dates will be proposed after consultation with the affected business area Manager and the Information Officer. Corrective action will be tracked until adequately resolved. The remedial action taken must mitigate the risk of a similar incident re-occurring.

16. APPLICATION FOR ISSUING CODE OF CONDUCT

Application for issuing code of conduct

A private or public body which is sufficiently representative of any class of bodies, or of any industry, profession, or vocation that wishes to apply for the issuing of a code of conduct in terms of section 61(1)(b) of the Act, must submit an application to the Regulator on Form 3. (Available on request)

17. POPI COMPLIANT PROCEDURE

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. The organisation takes all complaints very seriously and will address all POPI-related complaints in accordance with the Following procedure:

- POPI complaints must be submitted to the organisation in writing. Where so required, the data subject will be provided with a "POPI Complaint Form".
- Where the complaint has been received by any person other than the Information Officer or Deputy Information Officer, that person will ensure that the Full details of the complaint reach the Information Officer or Deputy Information Officer within 1 working day.
- The Deputy Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
- The Deputy Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Deputy Information Officer will endeavour to resolve the complaint in a Fair manner and in accordance with the principles outlined in POPIA.
- The Deputy Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the organisation's data subjects.
- Where the Information Officer or Deputy Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer or Deputy Information Officer will consult with the organisation's governing body, and after the affected data subject(s) and the Information Regulator will be informed of this breach.
- The Deputy Information Officer will revert to the complainant with a proposed solution, with the option of escalating the complaint to the organisation's governing body within 7 working days of receipt of the complaint. In all instances, the organisation will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.

- The Deputy Information Officer's response to the data subject may comprise any of the following:
  - A suggested remedy for the complaint,
  - A dismissal of the complaint and the reasons as to why it was dismissed,
  - An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- Where the data subject is not satisfied with the Deputy Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
- The Information Officer or Deputy Information Officer will review the complaints process to assess the effectiveness of the procedure periodically and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI-related complaints.

18. SUBMISSION OF COMPLAINT

1. Any person who wishes to submit a complaint contemplated in section 74(1) of the Act must submit such a complaint to the Regulator on Part I of Form 5 (available upon request).
2. A responsible party or a data subject who wishes to submit a complaint contemplated in section 74 (2) of the Act must submit such a complaint to the Regulator on Part II of Form 5 (available upon request).

19. REGULATOR ACTING AS CONCILIATOR DURING INVESTIGATION

1. If, during the investigation of a complaint, the Regulator decides to act as a conciliator in terms of section 76(1) (b) of the Act, and convene a conciliation meeting, the Regulator must, as soon as it is practically possible, inform the data subject and the responsible party implicated in the complaint on Form 6 (available on request) of the following:
   a. The Regulator's decision to act as a conciliator in the matter, and
   b. The date, time and place of the conciliator meeting.
2. The Regulator
   a. May consolidate separate complaints, which are alleged to relate to the same interference with the protection of personal information by the same responsible party, to deal with the complaints in the same conciliation proceedings;
   b. Must ensure that all persons entitled to attend the conciliation meeting are notified within a reasonable time of the date, time and place of the meeting;
   c. May request all the relevant documentation relating to the complaint from the data subject and the responsible party; and
   d. May confer with the parties in person, by electronic communication means, or by any other means as is deemed appropriate.
3. Where a conciliation meeting fails to take place, the Regulator must arrange for an alternative date and notify the persons entitled to attend the conciliation meeting accordingly.
4. The Regulator must issue a conciliation certificate on Form 7 (available on request) within a reasonable time after the date of the conclusion of the conciliation meeting.
5. If the complaint is not resolved, or either or both of the parties did not attend a conciliation meeting, the Regulator must proceed with the complaint as provided for in terms of section 76 of the Act.

20. PRE-INVESTIGATION PROCEEDINGS OF REGULATOR

1. If the Regulator intends to investigate any matter contemplated in Chapter 10 of the Act, the Regulator must, in terms of Section 79 of the Act, notify the parties to whom the investigation relates of such intention on Part I of Form 8 (available on request) prior to conducting the investigation.
2. The Regulator must inform the responsible party to whom the investigation relates on Part II of Form 8 of the complaint, or the subject matter of the investigation, and must inform the responsible party of the right to submit a written response to the complaint or the subject matter of the investigation within the time allocated by the Regulator.

21. SETTLEMENT OF COMPLAINTS

1. If the appears form a complaint or any written reply to the complaint under section 79(b)(ii) of the Act or during a conciliation meeting, that it may be possible to secure a settlement between the parties and if appropriate, satisfactory assurance as contemplated in section 80 of the Act, the Regulator may confer with the parties in person, by electronic communication means, or by any other means as is deemed appropriate to endeavour to obtain a settlement and if appropriate, satisfactory assurances as contemplated in Section 80 of the Act.
2. If, during the process referred to in sub-regulation (1), the Regulator decides to convene a settlement meeting, the Regulator must, as soon as it is practically possible, inform the data subject and the responsible party on Form 9 (available on request) of the date, time and place of the settlement meeting.
3. For the purpose of settlement proceedings, the Regulator has the same powers as a conciliator contemplated in sub-regulation {2) to (3) of Regulation 8.
4. The Regulator must issue a settlement certificate on Form 10 (available on request) within a reasonable time after the date of the conclusion of the settlement meeting.
5. If no settlement and assurance are secured or if either or both of the parties do not wish to attend a settlement meeting, the Regulator must proceed with the matter as provided for in terms of section 76 of the Act.

22. ASSESSMENT

1. A request for an assessment in terms of section 89 (1) of the Act must be submitted to the Regulator on Part 1 of Form 11 (available on request).
2. The Regulator must inform the requester on Part II of Form 11 (available on request) if it has decided to conduct an assessment on -
   a. Its own initiative; or
   b. As requested in terms of sub-regulation (1), within a reasonable time from the date that the decision was made.
3. The period of assessment will be determined by the Regulator on a case-by-case basis.
4. The Regulator must notify the requester or the responsible party (if not the requester) of any decision made, or action taken, or view formed on Form 12 (available on request) within a reasonable time from the date that the decision was made or action taken or view formed.

23. INFORMING THE PARTIES OF DEVELOPMENTS REGARDING INVESTIGATION

1. During the course of an investigation, the Regulator must, within a reasonable time from the date of a decision being made or action being taken -
   a. Keep the complaint, the data subject (if not the complaint) and the responsible party informed of the developments of the investigation; and
   b. Inform the complainant, data subject (if not the complaint) and the responsible party of the result of the investigation.
2. The notifications contemplated in sub-regulation (1) must be served at the designated addresses of the complaint, the data subject and the responsible party advising -
   a. On Form 13 (available on request), it is stated that an enforcement notice will not be issued in terms of section 94 (a) of the Act;
   b. From 14 (available on request), the complaint has been referred to the Enforcement Committee in terms of Section 92 of the Act;
   c. On Form 15 (available on request), an enforcement notice has been served in terms of section 95 of the Act;
   d. On Form 16 (available on request), it is stated that an enforcement notice has been cancelled or varied in terms of section 96 of the Act;
   e. On Form 17 (available on request), an appeal has been lodged against an enforcement notice for cancellation or variation of the notice in terms of section 97 of the Act;
   f. On Form 18 (available on request), that an appeal against an enforcement notice has been allowed and that an enforcement notice has been substituted in terms of section 98 of the Act; or
   g. On Form 19 (available on request), it is stated that an appeal has been dismissed in terms of section 98 of the Act.

T 0861 555 119
E hello@vitallegal.co.za
vitallegal.co.za
Canal Edge 2, Ground Floor, Entrance A,
Tyger Waterfront, Bellville, Cape Town

Reg. No. 2013/150097/07
Vital Legal Services (Pty) Ltd is an authorised Financial Services Provider, FSP No. 40817

Vital Legal Services (Pty) Ltd products are underwritten by GuardRisk Insurance Company, a licensed non-life insurer and authorised Financial Services Provider, FSP No. 75