TIBER POPIA & PAIA POLICY MANUAL

TIBER POPIA & PAIA POLICY MANUAL

Table of Contents

Tiber POPIA policy & privacy notice Guidelines

Who are the role players?

The data subject: a person that the personal information belongs to or is about. Under POPIA, a data subject can be a natural person (i.e., an individual) or a juristic person (i.e., legal entities such as companies), and therefore measures need to be put in place to protect the personal information of both individuals and legal entities.

The responsible party: a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

The operator: a party who processes personal information on behalf of the responsible party under a contract or mandate. POPIA sets out eight conditions that businesses must comply with when processing the personal information of data subjects. These 8 conditions are the foundational principles of POPIA that, when complied with, ensure that a data subject's personal information is being processed lawfully.

Regulator: The Information Protection Regulator established by POPI.

What is meant by ''Personal Information''?

Below is the definition of Personal Information as stated in the POPI Act:

"Personal information means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

1. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person.
2. information relating to the education or the medical, financial, criminal or employment history of the person.
3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other assignment to the person.
4. the biometric information of the person.
5. the personal opinions, views, or preferences of the person.
6. 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.
7. the views or opinions of another individual about the person; and
8. 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;"

Both INDIVIDUALS and COMPANIES are included in the ambit of Personal Information

What is a privacy notice?

A privacy notice explains how we obtain, use and disclose your personal information, in accordance with the requirements of the Protection of Personal Information Act ("POPIA")

It states what personal data we collect from your, why, and how we keep it private.

What is processing?

- Processing is ANY activity concerning personal information, e.g.
  The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alternation, consultation or use.
- Dissemination by means of transmission, distribution or making available in any other form.
- Merging, linking, blocking, degradation, erasure, or destruction of information.

Not covered:

- Purely household activity
- Information that has been de-identified, (*cannot identify a person*)

It is not ‘’personal information’’ if the information is already in the public domain or is not used, or intended to be used, in trade or commerce.

POPI compliance by the Company / Information Officer:

The role of the Information Officer.

- Clearly understand the data processing activities that the Company engages in.
- Training of relevant staff should be conducted on a continuous basis to ensure that staff are trained to understand the impact of POPI on their area of focus within the company.
- Consider whether appropriate written contracts are in place with *Third parties* for whom personal data is processed, or to whom the processing of personal data is outsourced.
- Evaluate the security measures in place to keep personal data always secure.
- The terms under which intra-group transfers of personal data are made.
- Consider in detail, the cross-border transfer of personal data; and review internal procedures ensuring continued compliance with POPI and the effective and efficient handling of enquiries and complaints by individuals.

- Ensure that the legitimate grounds for collecting and using personal data collected to ensure that data is not used in ways that have unjustified, adverse effects on the individuals concerned.
- The lawful purpose for which data are being collected to ensure that the data shall not be further processed in any manner that is contrary to that purpose or the purposes for which that data were collected.
- The extent of information that is required for the purpose as intended and to ensure that they collect adequate and relevant information and prevent any excessive information collection.
- The information retention periods and requirements applicable together with destruction processes and procedures.
- The rights of individuals, I.E., data subjects, in terms of POPI.

Other compliance issues:

- Security measures required to prevent the unauthorised or unlawful processing of personal data/access to personal data, including accidental loss or destruction or damage to personal data.
- If you transfer data outside of the country, to understand the roles, duties and responsibilities of all parties involved; and
- What processes and procedures should be in place to ensure that data is kept up to date and current and accurate at all times.

POPIA COMPLIANCE

8 CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

The Protection of Personal Information Act ("POPIA") regulates how personal information is collected, used, stored, retained, destroyed, and generally processed from the moment of collection until the moment of destruction, keeping data subjects' right to privacy of their own personal information at the forefront of how organisations use, share, and handle their information.

1. Accountability - the Responsible Party has an obligation to ensure that there is compliance with POPI in respect of the Processing of Personal Information.

2. Processing limitation - Personal Information must be collected directly from a Data Subject to the extent applicable; must only be processed with the consent of the Data Subject and must only be used for the purposes for which it was obtained. Data subject consent is required, *but not if*:

- Would prejudice lawful purpose, or
- Information is contained in public record.

3. Purpose specification - Personal Information must only be processed for the specific purpose for which it was obtained and must not be retained for any longer than it is needed to achieve such purpose.

4. Further processing limitation - further processing of Personal Information must be compatible with the initial purpose for which the information was collected.

5. Information quality - the Responsible Party must ensure that Personal Information held is accurate and updated regularly and that the integrity of the information is maintained by appropriate security measures.

6. Openness - there must be transparency between the Data Subject and the Responsible Party.

7. Security safeguards - a Responsible Party must take reasonable steps to ensure that adequate safeguards are in place to ensure that Personal Information is being processed responsibly and is not unlawfully accessed.

8. Data Subject participation - the Data Subject must be made aware that their information is being processed and must have provided their informed consent to such processing.

Retain records for required periods.

- Personal information must be destroyed, deleted or de-identified as soon as the purpose for collecting the information has been achieved.
- However, as record of the information must be retained if an organisation has used it to decide about the data subject, the record must be kept for a period long enough for the data subject to request access to it. Most HR, Financial documents should be retained for a period of 5-7 years.

Special Personal Information:

- Religious or political beliefs
- Race or ethnic origin
- Trade union membership
- Political opinions
- Health, sexual life
- Criminal behavior

TIBER - CONSENT TO PROCESS PERSONAL INFORMATION

in respect of Employee Information

A. USE OF PERSONAL INFORMATION

1. The Company is required to process personal data relating to you as the employee within the framework of performing the employment contract and/or provisions ensuing from or in relation to the employment relationship. Tiber is required to use your personal information for the purpose of its personnel and payroll records and to comply with its statutory obligations, including but not limited to statutory contributions, PAYE contributions, to maintain and improve effective personnel records, including payroll records and compliance with statutory obligations, to administer employee benefits, and to administer programmes and schemes with respect to training and development, performance appraisals, compensation, planning and organisation.

   For these purposes and to comply with its statutory obligations, you hereby agree to the processing and storage of your personal information by the Company as well as to the transmission of information as required. Tiber will process the personal information in a proper and careful manner. Furthermore, the Company will take appropriate technical and organisational measures to sufficiently safeguard personal information and to preserve the confidential nature of the Employee's personal information in compliance with the Protection of Personal Information Act.

   Privacy Policy - Tiber is committed to protecting its employee's privacy and recognises that it needs to comply with statutory requirements in collecting, processing, and distributing of personal information. The Constitution of the Republic of South Africa provides that everyone has the right to privacy and the Protection of Personal Information Act 4 of 2013 ("POPI") includes the right to protection against unlawful collection, retention, dissemination and use of personal information. In terms of section 18 of POPI, if personal information is collected, Tiber, as responsible party, must take reasonably practical steps to ensure that the data subject is made aware of the information being collected.

2. In accordance with POPI, Tiber hereby provides the following information:

2.1 ***Type of Information***:

Curriculum Vitae, ID, Qualifications, and related information required for payroll records and to comply with its statutory obligations for purposes of employment to ensure the appropriate cover of the employee as required by these parties.

2.2 ***Nature/category of Information***:

Personal information for employment purposes.

2.3 ***Purpose***:

Required for purposes of employment of the employee to ensure the contractual obligations of the employee and the Company, and/or for protection of the legitimate interests of the parties and/or in terms of legislation.

2.4 ***Source***:

From the employee (data subject) directly.

2.5 ***Tiber details* (Responsible party):**

Available on the TIBER website.

2.6 ***Voluntary/Mandatory***:

The employee is required to provide the information voluntarily and understands that same is mandatory for purposes of employment, health cover, including disability and funeral cover of the employee.

2.7 ***Legal Requirement***:

Tiber may be required, directly or indirectly, in terms of the Labour Relations Act 66 of 1995 (as amended), The Basic Conditions of Employment Act 75 of 1997 (as amended), The Skills Development Levy Act of 1999, the Employment Equity Act of 1998 and other Acts to collect the information to report to the Ministry of Labour or other Government structures and for responsible record keeping and statistical purposes.

2.8 ***Contractual Requirement*:**

The information is required in terms of the employee agreement between the employee and Tiber as well as Payroll, third-party consultants / service providers.

2.9 ***Consequences of failure to provide***:

Failure to provide the information will result in a failure of contractual employment. This will result in the employer /employee not complying with all legislative requirements.

2.10 ***Recipients of personal information***:

Tiber, Payroll, third-party consultants / service providers. Where necessary the information may be shared with other similar institutions.

2.11 ***Access and right to amend***:

The employee has the right to access and amend his/her personal information at any reasonable time.

2.12 ***Right to object****:*

The employee is entitled to object to the use of information. However, such objection may lead to the employment agreement being terminated as the information is required for valid reasons.

2.13 ***Complaints***:

All complaints regarding the use of personal information may be directed to the Information Regulator.

B. CONSENT

1. The employee (as data subject), by signing this document, hereby consents to the use of his/her personal information contained herein and confirms that:

   1.1 the information is supplied voluntarily, without undue influence from any party and not under any duress.

   1.2 the information which is supplied herewith is mandatory for the purposes of this agreement and that without such information, Tiber cannot enter into agreement with the employee.

   1.3 failure to provide the information will result in failure of contractual employment.

2. The employee acknowledges that he/she is aware thereof that he/she has the following rights about such personal information which is hereby collected. The right to:

   2.1 access the information at any reasonable time for purposes of rectification thereof.

   2.2 object to the processing of the information in which case this agreement will terminate in accordance with the provisions contained herein.

   2.3 lodge a complaint to the Information Regulator.

ACCEPTANCE

I,_____hereby agree to the terms and conditions as outlined above.

SIGNED:	DATE:

The data mapping template forms the basis for managing resources, accountability and protecting the rights of individuals. It provides the foundation for effective recordkeeping within the Company and demonstrates to employees and stakeholders its importance. The policy will help to communicate expectations, procedures and responsibilities, and serve as a mandate for recordkeeping activities.

TIBER CONSTRUCTION

Date:
Department:
Function:

DATA FLOW MAPPING

Function to be Mapped	**Type, nature, and category of data to be Mapped** (e.g. Invoice, ID, Acc no.)	**Source of collection** (e.g., Received from Employee, supplier, recruiter, client)	**What is the purpose of this information** (e.g., For compliance, for safety, budgeting, for performance management)	**Basis for lawful processing** 1. Contract 2. Legal Obligation 3. Employee's interest 4. Company's interests 5. Consent	**Method of processing information**						**How long is the information kept?** (e.g., 5 years or 7 years by law)	**How is this information destroyed and by who?** (e.g. Shredded from files, deleted off the server)
					Form of information being used. (e.g., Digital Physical or portable)	**Who uses this information?** (e.g., Internal staff or a third party)	**Who is this information shared with?** (e.g., SHE Reps, third party, accounts)	**Cross border transfer** (e.g.,' transactions or payments made company's in other countries)	**How is this information stored and where? ?** (e.g., On site, in the office in a locked cupboard, on a secure server)	**Who has access to this information & security?** (e.g., Office staff, the office is access controlled)		

SECURITY IMPLEMENTATION CHECKLIST

Items	Date	Comment	Recommended Intervention
Premises **Site:** _____			
Inspection of physical security & access			
Access control, cards, tags & biometrics			
Alarm and deactivation codes			
Armed response			
No go areas demarcated			
Risk analysis of security issues			
Filing and physical record keeping			
Locked offices and cabinets			
No-go areas			
Proper disposal of records/files/hard copy - shredding policy			
Work/document flow - data remains secure			
File integrity & lockup			
Staff			
Keys to authorized employees only			
Alarm codes			
Area specific access			
Staff are aware of their POPIA obligations			

Third party processing			
External operators all have written contracts			
External operators are aware of data usage security and limitations			
External operator confidentiality requirements			
Inspection of 3rd parties' premises, systems & compliance (monthly)			
IT & Data			
Computers physically secured			
Password policy			
Back-up policy & schedule			
Personal appointed to manage backups			
Off-site storage			
Proper disposal of damaged devices/data drives			
Network, internet & www security			
Mobile Devices			
Private devices not permitted to sync on networks			
Laptop - password secured			
Theft prevention strategy			
Security Breaches			
Any loss of data / security breach the regulator			
Any loss of data / security breach the data subject			

TIBER INCIDENT RESPONSE PLAN

What is incident response?

Incident response is an approach to handling security breaches. The aim of incident response is to identify the scope of the events, contain the damage, and mitigate or eradicate the root cause of the incident. An incident represents a change in security posture potentially in breach of law, policy, or unacceptable act that concerns information assets, such as networks, computers, or smartphones – which may or may not be materially reportable.

Here are several types of significant security incidents caused by malicious external threat actors that require organized incident response.

Phishing and social engineering

These attacks often involve manipulating individuals into disclosing confidential information, such as passwords or credit card numbers.

Social engineering uses psychological manipulation to trick people into making security mistakes or giving away sensitive information. Examples can range from emails claiming to be from a trusted source to phone calls, to even physical impersonations.

DDoS attacks

Distributed Denial of Service (DDoS) attacks are a type of incident that floods a network, system, or server with traffic to overwhelm it and make it inaccessible to users. These attacks can be crippling to an organization dependent on their website or system for daily activity, causing significant downtime, and potentially leading to loss of revenue and customer trust – or even physical harm (if in healthcare or manufacturing, depending on the system.).

DDoS attacks can be particularly hard to defend against because they are performed by botnets, which might have thousands or millions of compromised computers attacking the target simultaneously. This type of attack is often used as a smokescreen for other malicious activities, distracting security teams while other attacks or trojans are employed.

Supply chain attacks

Software supply chain attacks, also known as value-chain or third-party attacks, occur when someone infiltrates our system through an outside partner or supplier who has access via network connection to our systems and data. This type of cyberattack can be particularly damaging because it can bypass traditional security measures and give the attacker deep access to sensitive data and intellectual property.

Ransomware

Ransomware is a type of malicious software that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. Ransomware attacks can lead to significant business disruption and financial loss if critical systems or data are impacted.

Insider threats

Insider threats are security threats that originate from within the organization. These may come from both careless and disgruntled employees, contractors, or anyone else who has been granted insider access to the company's network and data.

These threats can be particularly challenging to manage and detect because these individuals often already have legitimate access to the company's systems. This type of incident can lead to significant damage, including intellectual property theft, financial fraud, and damage to the company's reputation.

The six steps of Incident Response Plan

1. Preparation

Here are steps your incident response team should take to prepare for cybersecurity incidents:

- Review the tools needed to defend against each of these incident types and centralize their management.
- Review security policies and conduct risk assessments modelled against external attacks, internal misuse/insider attacks, and situations where external reports of potential vulnerabilities and exploits.
- Prioritize known security issues or vulnerabilities that cannot be immediately
- Develop a communication plan for internal, external, and (if necessary) public breach reporting.
- Outline the roles, responsibilities, and procedures of the immediate incident response team, and the extended organizational awareness, operational, or training needs.

2. Identification

Decide what criteria calls the incident response team into action, and follow the information gathering document for the focal point

When an incident is isolated, it should be alerted to the incident response team. Team members coordinate the appropriate response to the incident:

- Identify and assess the incident and gather evidence.
- Decide on the severity and type of the incident and escalate, if necessary.
- Document actions taken, addressing "who, what, where, why, and how." This information will be used later as evidence if the incident reaches a court of law.

3. Containment

Once your team isolates a security incident, the aim is to stop further damage. This includes:

- **Short-term containment** — an instant response, so the threat doesn't cause further damage.
- **System backup** — you should back up all affected systems before you wipe and reimage them to acquire a "current state" or forensic image.
- **Long-term containment** — While making temporary fixes to replace systems that have been taken down to image and restore, rebuild clean systems so you can bring them online in the recovery stage. Take measures to prevent the incident from recurring or escalating install any security patches on affected and associated systems, remove accounts and backdoors created by attackers, alter firewall rules, and change the routes to null route the attacker address, etc.
- **Create scope documentation** — It is important to know precisely which credentials, service accounts, endpoints, servers, etc. were involved in the incident. It's important to establish a place for storing disk images, lists, and reports for a clean chain of investigation and evidence preservation.

4. Eradication

Contain the threat and restore initial systems to their initial state, or close to it. The team should isolate the root cause of the attack, remove threats and malware, and identify and mitigate vulnerabilities that were exploited to stop future attacks.

To stop the bleeding and limiting the amount of data that is exposed\, the following can be done:

- Identify and fix all affected hosts, including hosts inside and outside your organization
- Isolate the root of the attack to remove all instances of the software
- Conduct malware analysis to determine the extent of the damage
- See if the attacker has reacted to our actions – check for any new credentials created or permission escalations going back to the publication of any public exploits or POCs
- Make sure no secondary infections have occurred, and if so, remove them
- Allow time to make sure the network is secure and that there is no further activity from the attacker(s)

Ensure your team has removed malicious content and checked that the affected systems are clean. For example, if the attacker used a vulnerability, it should be patched, or if an attacker exploited a

5. Recovery

The purpose of this phase is to bring affected systems back into the production environment carefully to ensure they will not lead to another incident. Always restore systems from clean backups, replacing compromised files or containers with clean versions, rebuilding systems from scratch, installing patches, changing passwords, and reinforcing network perimeter security, (E.g., boundary router access control lists, firewall rulesets, etc.)

Decide how long you need to monitor the affected network and endpoint systems, and how to verify that the affected systems are functioning normally. Calculate the cost of the breach and associated damages in productivity lost, human hours to troubleshoot and take steps to restore, and recover fully.

6. Lessons Learned

After any incident, it's important to hold a debriefing or lessons learned meeting to capture what happened, what went well, and evaluate the potential for improvement. The incident response team and stakeholders should communicate to improve future processes. Complete documentation that couldn't be prepared during the response process. The team should identify how the incident was managed and eradicated.

The Information officer L. Chetty as well as the Netsurit IT Consultant must be notified. immediately in the event of a Data security breach as listed above or when mistakenly forwarding a confidential e-mail to the incorrect recipient or clicking on a phishing e-mail.

Any employee who has knowledge of any tampering with circumvention of or breach of security or security measures shall notify either their supervisor or the Security Division immediately.
Investigations of alleged violations of this policy will be conducted under the direction of the Security company and HR Director/Information officer.

At the conclusion of the investigation, any employees found to be in violation of this policy will be subject to disciplinary action, up to and including termination of employment.
Tiber's Security Incident Management system includes lodging criminal charges, polygraph tests, investigation of all incidents reported via the whistleblowing channel.

TIBER CONSTRUCTION PROPRIETARY LIMITED

Registration Number: 1988/005498/07

("the Company")

MANUAL FOR ACCESS TO INFORMATION

In terms of

SECTION 51 OF THE PROMOTION OF ACCESS TO INFORMATION ACT 2000, NO 2 OF 2000

("the Act")

TIBER CONSTRUCTION PROPRIETARY LIMITED

Registration Number: 1988/005498/07

INTRODUCTION

The purpose of the Promotion of Access to Information Act, 2000 ("the Act") is to give effect to the constitutional right of access to any information held by the State and any information that is held by another person and that is required for the exercise or protection of any rights; to provide that the Information Regulator, established in terms of the Protection of Personal Information Act, 2013, must exercise certain powers and perform certain duties and functions in terms of this Act; and to provide for matters connected therewith.

Recognizing that the system of government in South Africa before 27 April 1994, amongst others, resulted in a secretive and unresponsive culture in public and private bodies which often led to an abuse of power and human rights violations. Section 8 of the Constitution provides for the horizontal application of the rights in the Bill of Rights to juristic persons. While section 32(1)(a) of the Constitution provides that everyone has the right of access to any information held by the state. Section 32(1)(b) of the Constitution provides for the horizontal application of the right of access to information held by another person to everyone when that information is required for the exercise or protection of any rights. Bearing that in mind the State must respect, protect, promote, and fulfil, at least, all the rights in the Bill of Rights which is the cornerstone of democracy in South Africa. The right of access to any information held by a public or private body may be limited to the extent that the limitations are reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom as contemplated in section 36 of the Constitution. Reasonable legislative measures may, in terms of section 32(2) of the Constitution, be provided to alleviate the administrative and financial burden on the State in giving effect to its obligation to promote and fulfil the right of access to information.

AND IN ORDER TO -

- Foster a culture of transparency and accountability in public and private bodies by giving effect to the right of access to information.
- Actively promote a society in which the people of South Africa have effective access to information to enable them to exercise and protect all their rights more fully.

Tiber Construction (Pty) Ltd conducts business as a construction company.

SECTION 1 (Information required under Section 51 (1)(a) of the Act)

Name of company	Tiber Construction (Pty) Ltd
Company Registration Number	1988/005498/07
Postal Address	PO Box 857, Wendywood, 2144
Physical Address	12 Desmond Street, Kramerville, Sandton, 2146
Telephone Number	011 430 7700
Facsimile Number	011 430 7999
E-mail Address	tiber@tiber.co.za
Chief Information Officer	Leonora Elaine Chetty

SECTION 2 (Information required under Section 51 (1)(b) of the Act)

A Guide has been compiled in terms of Section 10 of PAIA by the Human Rights Commission. It contains information required by a person wishing to exercise any right, contemplated by PAIA. It is available in all the official languages. The Guide is available for inspection, *inter alia*, on its website at www. sahrc.org.za.

SECTION 3 (Information required under Section 51(1)(d) of the Act)

Records are kept in accordance with such other legislations as is applicable which includes, but is not limited to, the following:

Labour Relations Act 66 of 1995
Employment Equity Act 55 of 1998
Basic Conditions of Employment Act 75 of 1997
Compensation for Occupational Injuries and Disease Act 130 of 1993
Unemployment Insurance Act 63 of 2001
Skills Development Act 9 of 1999
Skill Development Levies Act 9 of 1999
Occupational Health and Safety Act 85 of 1993
Regional Services Councils Act 109 of 1985
Companies Act, 2008 (Act No 71 of 2008)
Income Tax Act 58 of 1962
Value Added Tax Act 89 of 1991

SECTION 4 (Information required under Section 51(1)(e) of the Act)

Subjects and categories of records held by the company:

- Identity numbers
- Dates of birth
- Telephone numbers
- E-mails
- Addresses
- Banking details
- Bank account numbers
- BEE Certificates
- Invoices

COMPANIES ACT RECORDS:
Documents of Incorporation
Memorandum of Incorporation
Minute books
Share register and other statutory registers
Records relating to all documents lodged with CIPC
FINANCIAL RECORDS:
Annual Financial Statements
Tax returns
Accounting records
VAT records
Banking records
Asset register
Lease Agreements
Invoices

SECTION 5 (Information required under Section 51(e) and Section 53 of the Act)

The Request procedure:

FORM OF REQUEST: (SEE ATTACHED AT THE END OF THIS MANUAL)

The requester must use the prescribed form to make the request for access to a record. This must be made to the head of the private body/Information Officer. This request must be made to the address, fax number or electronic mail address of the body concerned. The requester must provide sufficient detail on the request form to enable the head of the private body / Information Officer to identify the record and the requester. The requester should also indicate which form of access is required. The requester should also indicate if any other manner is to be used to inform the requester and state the necessary particulars to be so informed. The requester must identify the right that is sought to be exercised or to be protected and provide an explanation of why the requested record is required for the exercise or protection of that right. If a request is made on behalf of another person, the requester must then submit proof of the capacity in which the requester is making the request to the satisfaction of the head of the private body.

FEES:

A requester who seeks access to a record containing personal information about that requester is not required to pay the request fee. Every other requester, who is not a personal requester, must pay the required request fee:

The head of the private body must notify the requester (other than a personal requester) by notice, requiring the requester to pay the prescribed fee (if any) before further processing the request. The fee that the requester must pay to a private body is R50. The requester may lodge an application to the court against the tender or payment of the request fee. If the request is granted then a further access fee must be paid for the search, reproduction, preparation and for any time that has exceeded the prescribed hours to search and prepare the record for disclosure.

AVAILABILITY OF RECORDS AND THE MANUAL:

The required record and/or manual is available for inspection during office hours at the offices, as disclosed on page 1. Copies of the manual are also available from the SAHRC.

Signed at Kramerville on this 19th day of May 2021, by the authorised representative:

JCorreia

Mr. Jose Correia

POPIA OPERATOR AGREEMENT (Addendum to Principal agreement)

1. Introduction

1.1. The parties entered into the Principal Agreement on _____.

1.2. The parties agree that the Service Provider shall act as an Operator as defined in POPIA in respect of the Protected Data.

1.3. The parties hereby agree to enter into this Agreement in compliance with their duties and obligations in terms of section 20 of POPIA.

2. Definitions and Interpretation

2.1. Unless otherwise defined herein, terms and expressions used in this Agreement shall have the following meaning:

2.1.1. **"Agreement"** means this Operator Agreement.

2.1.2. **"Client"** means _____.

2.1.3. **"Data Breach"** means any security compromise as envisaged by section 22 of POPIA.

2.1.4. **"Data Subject"** means the natural or juristic person to whom relevant personal information relates.

2.1.5. **"Information Regulator"** means the Information Regulator established in terms of section 39 of POPIA.

2.1.6. **"Operator"** means a person or entity who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

2.1.7. **"Personal Information"** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person.
(b) information relating to the education or the medical, financial, criminal or employment history of the person.
(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other assignment to the person.
(d) the biometric information of the person.
(e) the personal opinions, views, or preferences of the person.
(f) 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.
(g) the views or opinions of another individual about the person; and
(h) the name of the person if it appears with other personal information relating to the person

or if the disclosure of the name itself would reveal information about the person.

2.1.8. **"POPIA"** means the Protection of Personal Information Act, 4 of 2013. Any reference to POPIA shall include all regulations issued in terms of POPIA and all directives and other guidance documents issued by the Information Regulator.

2.1.9. **"Principal Agreement"** means the agreement entered between the Client and the Service Provider on _____ with respect to _____ service.

2.1.10. **"Processing"** means any operation or activity or any set of operations, whether by automatic means, concerning personal information, including—
(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use.
(b) dissemination by means of transmission, distribution or making available in any other form; or
(c) merging, linking as well as restriction, degradation, erasure, or destruction of information.

2.1.11. **"Protected Data"** means all Personal Information supplied to the Service Provider by the Client to enable it to perform its duties and obligations in terms of the Principal Agreement.

2.1.12. **"Responsible Party"** means public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

2.1.13. **"Services"** means the services that the Service Provider provides to the Client defined in the Principal Agreement.

2.1.14. **"Service Provider"** means _____; and

2.1.15. **"Special Personal Information"** means personal information as referred to in section 26 of POPIA.

2.2. When any number of days is prescribed in this Agreement, same shall be reckoned exclusively of the first and inclusively of the last day unless the last day falls on a Saturday, Sunday, or public holiday, in which event the last day will be the next business day; and

2.3. The rule of construction that a contract shall be interpreted against the Party responsible for the drafting or preparation of the contract, shall not apply.

3. Operator and Responsible Party

3.1. The parties agree that, in respect of the Protected Data, the Client shall be the Responsible Party and the Service Provider shall be the Operator.

3.2. The Service Provider shall comply with POPIA in connection with the processing of Protected Data and the exercise and performance of its rights and obligations under the Agreement.

4. Duties of Service Provider as Operator

4.1. In addition to the duties and responsibilities that is conferred on the Service Provider in the Principal Agreement and in this Agreement, the Service Provider shall:

4.1.1. Take reasonable steps to ensure that the Protected Data is complete, accurate and up to date, and not misleading.

4.1.2. Treat all Protected Data as confidential and not disclose it unless required by law or expressly authorised in writing by the Client.

4.1.3. Only process the Protected Data in accordance with this Agreement and in terms of the responsibilities in respect of compliance with POPIA delegated to it in terms of this Agreement.

4.1.4. Ensure that each of its subcontractors, employees, representatives, and agents is aware of requirements of this Agreement and the Service Provider's obligations in terms of POPIA.

4.1.5. Ensure that each of its subcontractors, employees, representatives, and agents have committed themselves in writing to keep the Protected Data confidential.

4.1.6. Keep the Protected Data secure; and

4.1.7. On a regular basis, but not less than once per year, assess, review and update security measures, and agree with the Client on all changes to security measures before promptly implementing such changes.

5. Instructions and Details of Processing

5.1. Insofar as the Service Provider processes Protected Data on behalf of the Client, the Service Provider shall:

5.1.1. only process Protected Data with the express written knowledge or consent of the Client.

5.1.2. unless required to do otherwise by law, process the Protected Data only on and in accordance with the Client's documented instructions as set out in the Principal Agreement and as updated from time to time by written agreement of the parties; and

5.1.3. if any applicable law requires it to process Protected Data other than in accordance with the Principal Agreement or further written agreement, shall notify the Client of any such requirement before processing the Protected Data, unless specifically so instructed by the Information Regulator.

5.2. The Service Provider shall ensure that each person, including, but not limited to subcontractors, employees, representatives, and agents acting under its authority and/or on its behalf, comply with the obligations set out in clause 5.1 above.

5.3. The processing that is carried out by the Service Provider in terms of this Agreement shall be in respect of Protected Data Information as agreed to in the Principal Agreement or as otherwise set out in writing from time to time.

5.4. The Personal Information that constitutes the Protected Data as set out in the Principal Agreement, may only be processed and accessed to comply with the obligations of the Service Provider in terms of the Principal Agreement.

6. Technical and Organisational Measures

6.1. The Service Provider shall implement and maintain, at its cost, appropriate technical and organisational measures to the reasonable satisfaction of the Client in relation to the processing of Protected Data by the Service Provider, to ensure that:

6.1.1. the processing meets the requirements of POPIA and that the rights of Data Subjects are protected.

6.1.2. security measures in respect of Protected Data processed by it, is appropriate to the risks that are presented by the processing, including but not limited to, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored, or otherwise processed; and

6.1.3. it can assist the Client in the fulfilment of its obligations to respond to Data Subject Requests relating to Protected Data.

6.2. The Service Provider shall, in respect of the Protected Data processed by it under the Agreement, ensure reasonably practicable technical and organisational security measures are implemented that would allow the Client to comply with the requirements of POPIA.

7. Subcontractors, Employees, Representatives and Agents

7.1. The Service Provider shall not subcontract any of its obligations in terms of the Principal Agreement or this Agreement to any other person or entity to act as Operator in carrying out any processing activities in respect of the Protected Data, without entering into an agreement with similar terms to this Agreement, with such subcontractor in compliance with POPIA.

7.2. The Service Provider shall ensure that all its subcontractors, employees, representatives, and agents who are entrusted to process the Protected Data, are subject to a binding written contractual obligations with the Service Provider not to disclose and to keep confidential the Protected Data, except in as far as such subcontractors, employees, representatives, and agents are not required by law to disclosure such Protected Data.

7.3. The Service Provider shall ensure that all subcontractors employees, representatives, and agents who process the Protected Data are reliable and have received adequate training on lawful processing in accordance with POPIA.

8. Assistance to the Client: Compliance and Data Subject Rights

8.1. The Service Provider shall, at its own cost:

8.1.1. promptly record and refer all Data Subject Requests it receives to the Client within three days of receipt of such request.

8.1.2. provide such information and cooperation, and take such action as the Client requests, in relation to a Data Subject request, within the timescales required by the Client; and

8.1.3. not respond to any Data Subject request or objection to processing or any complaint without the Client's prior written approval.

8.2. The Service Provider shall, at its own cost, provide to the Client such information, co-operation and other assistance as the Client may require, to ensure that the Client is able to comply with its obligations in respect of the Protected Data as required by POPIA, including, but not limited to:

8.2.1. security measures in place.

8.2.2. data protection impact assessments done and the results thereof; and

8.2.3. any remedial action taken and/or notifications in response to any Personal Data Breach and/or complaint.

8.3. The Client is responsible to notify affected Data Subjects and the Information Regulator of any Data Breaches reported to it by the Service Provider. The Service Provider shall under no circumstances without the prior written consent of the Client notify affected Data Subjects or the Information Regulator of any Data Breach.

9. Cross Border Transfers

9.1. The Service Provider shall not transfer any Protected Data to any location or recipient outside the borders of South Africa without the explicit prior written consent of the Client.

9.2. For avoidance of doubt storing the Protected Data on cloud servers not located within the borders of south Africa, shall be regarded as cross border transfer.

10. Records, Information and Audit

10.1. The Service Provider shall maintain complete, accurate and up to date written records of all processing that it carries out on behalf of the Client in respect of the Protected Data, containing sufficient information. Such records shall be supplied to the Client on request within a reasonable time.

10.2. The Service Provider shall:

10.2.1. allow for, and participate in, audits, including inspections, conducted by the Client or another auditor mandated by the Client for the purpose of ensuring compliance by the Service Provider with the obligations under POPIA that is delegated to it in terms of this Agreement; and

10.2.2. provide reasonable access for the Client or its delegated auditor to the facilities, equipment, premises, and sites on which Protected Data and/or are whether owned or controlled by the Service Provider, provided that the Client shall give the Service Provider reasonable prior notice of such audit and/or inspection.

10.3. The Service Provider shall promptly remedy, at its own cost and expense, all data protection and security issues found by the Client and reported to the Service Provider that may reveal a breach or potential breach by the Service Provider of its obligations as defined in this Agreement.

11. Notification of Data Breach or Complaints to the Client

11.1. The Service Provider shall, where it suspects or believes that the Protected Data has been accessed or acquired by unauthorised persons or used in a manner inconsistent with the contract or POPIA:

11.1.1. notify the Client of the Data Breach immediately, but no later than one working day after becoming aware of the Data Breach: and

11.1.2. provide the Client as soon as possible with such details as the Client reasonably requires regarding the nature of the Data Breach, to enable the Client to comply with its reporting obligations in terms of POPIA, any investigations it has conducted into such Data Breach by the Service Provider and any technical and organisational measures taken to address the cause of the Data Breach.

11.2. The Service Provider shall as soon as possible, but no later than two working days, after it has received any complaint about a potential Data Breach or objection to the processing of Personnel Information, inform the Client thereof, providing full details to allow the Client to take appropriate action.

12. Deletion or return of Protected Data

12.1. The Service Provider shall without delay, at the Client's written request, either securely delete, or securely return, all the Protected Data to the Client in such format as the Client reasonably requests:

12.1.1. on the termination of the Principal Agreement; or

12.1.2. once processing by the Service Provider of any Protected Data is no longer required for the purpose of the Service Provider's performance of its relevant obligations under the Agreement.

whichever event takes place first, and securely delete existing copies, in so far as retention of records are not required by law, and, where so required, inform the Client of any such requirement and period of retention.

13. Indemnification and Liability

13.1. The Client hereby indemnifies and holds the Service Provider harmless against all costs, claims, damages, or expenses incurred by the Service Provider or for which the Service Provider may become liable due to any failure by the Client or its subcontractors, employees, representatives and/or agents to comply with the obligations under this Agreement or with its obligations in terms of POPIA in respect of the Protected Data.

13.2. The Service Provider hereby indemnifies and holds the Client harmless against all costs, claims, damages, or expenses incurred by the Client or for which the Client may become liable due to any failure by the Service Provider or its subcontractors, employees, representatives and/or agents to comply with the obligations under this Agreement or with the obligations in terms of POPIA delegated to it in terms of this Agreement in respect of the Protected Data.

13.3. Notwithstanding the above, neither party shall be liable for any indirect or consequential damages of the other party, including, but not limited to, loss of revenue, loss of profit, loss of opportunity and loss of goodwill.

13.4. No limitation of liability shall apply in case of gross negligence or willful intent.

14. Domicilium

14.1. Any notice or other document to be served under this Agreement to a party may be to be served at its address set out below:

14.1.1. The Client

Physical address
Contact person
Contact number
Email address

14.1.2. The Service Provider

Physical address
Contact person
Contact number
Email address

14.2. Either party shall be entitled from time to time, by written notice to the other, to vary its domicile address to any other address within the Republic of South Africa, which is not a post office box.

14.3. All notices given in terms of this Agreement shall be in writing and any notice given by one party to the other (the addressee) which:

14.3.1. is delivered by hand during the normal business hours at the addressee's *domicile* shall be deemed to have been received by the addressee at the time of delivery.

14.3.2. is sent by electronic mail to the addressee's electronic mail address shall be deemed to have been received by the addressee on the 1st (first) business day after the date of transmission thereof.

14.4. Notwithstanding anything to the contrary contained or implied in this Agreement, a written notice or communication received by one of the parties from the other including by way of electronic transmission shall be adequate written notice or communication to such Party.

15. Governing Law and Jurisdiction

15.1. This Agreement will in all respects be governed by and construed under the laws of the Republic of South Africa.

15.2. The Parties hereby consent and submit to the exclusive jurisdiction of the South Gauteng High Court of the Republic of South Africa in any dispute arising from or in connection with this Agreement.

16. General

16.1. This Agreement constitutes the whole agreement between the Parties relating to the subject matter hereof.

16.2. No amendment or consensual cancellation of this Agreement or any provision or term hereof or of any agreement or other document issued or executed pursuant to or in terms of this Agreement and no settlement of any disputes arising under this Agreement and no extension of time, waiver or relaxation or suspension of any of the provisions or terms of this Agreement or of any agreement, or other document issued pursuant to or in terms of this Agreement shall be binding unless recorded in a written document signed by the parties (or in the case of an extension of time, waiver or relaxation or suspension, signed by the party granting such extension, waiver or relaxation). Any such extension, waiver or relaxation or suspension which is so given or made shall be strictly construed as relating strictly to the matter in respect whereof it was made or given.

16.3. No extension of time or waiver or relaxation of any of the provisions or terms of this Agreement or any agreement, bill of exchange or other document issued or executed pursuant to or in terms of this Agreement, shall operate as an estoppel against any party in respect of its rights under this Agreement, nor shall it operate so as to preclude such party thereafter from exercising its rights strictly in accordance with this Agreement, unless such extension of time or waiver or relaxation has been agreed in writing, as set out above.

16.4. No party shall be bound by any express or implied term, representation, warranty, promise or the like not recorded herein, whether it induced the contract and/or whether it was negligent or not, unless fraudulently made.

16.5. If any of the provisions of this Agreement are held to be invalid, the validity of the remainder of this Agreement shall not be affected and the rights and obligations of the parties shall be construed as enforced as if this Agreement did not contain the invalid term, and to this end, the provisions of this Agreement and the application thereof are hereby declared to be severable.

Signed on this _____ day of _____ 20__ at _____

_____ _____

For Client
Duly authorised

Witness

Signed on this _____ day of _____ 20__ at _____

_____ _____

For Service Provider
Duly authorised

Witness

Form 2
REQUEST FOR ACCESS TO RECORD

https://acrobat.adobe.com/id/urn:aaid:sc:EU:faa6cc35-ee6e-45b6-a330-c9b4ec8faa39