

PROTECTION OF PERSONAL INFORMATION – POPI POLICY AND COMPLIANCE

Selhurst Recruitment Consulting cc is committed to compliance with and adheres to, the Protection of Personal Information ACT (POPI) and confirms that we comply with this legislation.

Introduction

The POPI Act requires us to:

1. Sufficiently inform candidates/applicants/work-seekers (data subjects), hereafter referred to as candidates, the purpose for which we will process their personal information.
2. Protect our Information assets from threats, whether internal or external, deliberate, or accidental, to ensure business continuation, minimise business damage and maximise business opportunities.

This policy and compliance framework establishes measures and standards for the protection and lawful processing of personal information within our organisation and provides principles regarding the right of individuals to privacy and to reasonable safeguarding of their personal information.

The Information Officer is responsible for:

- Conducting a preliminary assessment.
- The development, implementation and monitoring of this policy and compliance framework.
- Ensuring that this policy is supported by appropriate documentation.
- Ensuring that documentation is relevant and kept up to date.
- Ensuring this policy and subsequent updates are communicated to all relevant parties.

Policy Principles

Principle 1: Accountability

- We must take reasonable steps to ensure that personal information obtained from candidates is stored safely and securely.
- This includes CV's, Resumes, References, Qualifications, Integrity Checks, and any other personal information that may be obtained for the purpose of candidate representation.

Principle 2: Processing limitation

- We will collect personal information directly from candidates.
- Once in our possession we will only process or release candidate information with their consent, except where we are required to do so by law. In the latter case we will always inform the candidate.

Principle 3: Specific purpose

- We collect personal information from candidates to enable us to represent them to our clients for the purpose of recruitment.

Principle 4: Limitation on further processing

- Personal information may not be processed further in a way that is incompatible with the purpose for which the information was collected initially. We collect personal information for recruitment, and it will only be used for that purpose.

Principle 5: Information quality

- We are responsible for ensuring that candidate information is complete, up to date and accurate before we use it. This means that it may be necessary to request candidates, from time to time (at least every 12 months), to update their information and confirm that it is still relevant. If we are unable to reach a candidate for this purpose their information will be deleted from our records.

Principle 6: Transparency/openness

- Where personal information is collected from a source other than directly from a candidate (e.g., social media) we are responsible for ensuring that the candidate is aware:
 - That their information is being collected.
 - Who is collecting their information by giving them our details.
 - Of the specific reason that you are collecting their information.

Principle 7: Security safeguards

- We will ensure technical and organisational measures to secure the integrity of personal information, and guard against the risk of loss, damage, or destruction thereof. Personal information must also be protected against any unauthorised or unlawful access or processing. We are committed to ensuring that information is only used for legitimate purposes with candidate consent and only by authorised employees of our agency.

Principle 8: Participation of individuals

- Candidates are entitled to know particulars of their personal information held by us, as well as the identity of any authorised employees of our agency that had access thereto. They are also entitled to correct any information held by us.

Operational Considerations

Monitoring

The Information Officer is responsible for administering and overseeing the implementation of this policy and, as applicable, supporting guidelines, standard operating procedures, notices, consents and appropriate related documents and processes. We will conduct periodic reviews and audits, where appropriate, to ensure compliance with this policy and guidelines.

Operating controls

We shall establish appropriate standard operating procedures that are consistent with this policy and regulatory requirements. This will include:

- Allocation of information security responsibilities and incident reporting.
- Data backup.

Policy compliance

Any breaches will be reported to the Information Regulator.

For Candidates:

By Submitting your information and application you hereby confirm:

- 1) That you have read and understood our POPI Policy.
- 2) That you have no objection to us retaining your personal information in our database for future matching.
- 3) Should suitable opportunities arise we will contact you and request your consent to submit your CV to a specific

client for a specific purpose.

4) That the information you have provided to us is true, correct and up to date.

If you have any additional questions about Selhurst Recruitment Consulting's collection and storage of data, please contact us at:

PO Box 2657
Cramerview
2060

Tel: +27 (0) 82 929 8750

Email: Laurence@selhurst.co.za

