PROTECTION OF PERSONAL INFORMATION ACT
POLICY and PROCEDURE MANUAL

LEGAL CAREERS (PTY) LTD
PO BOX 3319
Houghton
2041
Phone No: 011 447-5411
Email address - Information Officer: info@legalcareersza.co.za

Introduction

We are committed to compliance with The Protection of Personal Information (POPI) Act and will:

1. Sufficiently inform Data Subjects (candidates/applicants/work-seekers hereafter referred to as "Candidate/s"), the specific purpose for which we will collect and process their personal information;

2. Protect Personal Information from threats, whether internal or external, deliberate or accidental, to ensure business continuation, minimise business damage and maximise business opportunities.

3. Train consultants on the importance of privacy and personal data.

This Policy establishes measures, processes and standards for the protection and lawful processing of personal information.

The **Information Officer & Deputy Officer**, (B.Lindsay & J. Louw), are responsible for:

- Monitoring this policy;
- Ensuring that this policy is supported by appropriate processes and procedures;
- Ensuring that this policy and subsequent updates are communicated to relevant managers and staff where applicable.

All employees, are responsible for adhering to this policy and for reporting any security breaches or incidents to the Information Officer.

Service Providers that provide IT and/or Off-site Data Storage services, to our organisation have satisfied us that they provide adequate protection of data held by them on our behalf.

Policy Principles

Accountability for Data to be collected

- We shall take reasonable steps to safeguard all Data and Personal Information collected from Candidates for the purpose of Permanent or Temporary recruitment.

Processing Limitation/Purpose for Data Collection

- We will collect personal information directly from candidates.
- Personal Information from Social Networks and Job-seeker portals will be collected with express consent of the Candidate/s.
- Once in our possession we will process or further process 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.

How we obtain your personal data

We can collect this information in a number of ways:

- Directly from you when: you interview with us, email us, call us, or when you apply for a position (whether via our website, via third parties such as job boards, social media sites, or otherwise) in connection with a background or employment check or an employment reference (subject to your consent where required by law).
- Third parties, such as references supplied by former employers or agencies and information from criminal records checks permitted by law.
- Social media platforms (such as Facebook, Twitter, LinkedIn), company websites, and other publicly available sources, from a recruiting or other web site where you may have provided information about your work experience or interests.
- Personal information collected from candidates will be used to secure Permanent or Temporary employment on behalf of Candidates.

How we will use data about you

- Assess your skills, qualifications, and suitability for the role;
- Carry out background and reference checks, where applicable;
- Communicate with you regarding the recruitment process;
- Keep records related to our hiring processes;
- Comply with legal or regulatory requirements.

If you fail to provide personal data when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we may not be able to process your application further. For example, if we require references for an advertised vacancy and you fail to provide us with relevant details, we will not be able to take your application further.

Limitation on Further Processing

- Unless otherwise requested, personal information may not be further processed in a way that is incompatible with the initial purpose for which it was collected.

Information Quality

- We will requested confirmation from the candidate that their information is complete, up to date and accurate before we use it. We will regularly request candidates to update their information and confirm that we may continue to store/retain same.

Data Security

- We will implement sufficient measures to guard against the risk of unlawful access, loss, damage or destruction of personal information that is held;
    - Physically;
    - in our electronic data base;
    - by a Data Storage Service Provide;
    - in any electronic devices (that will be Password protected).
- Data encryption of storage devices will be installed.
- We are committed to ensuring that information is only used for legitimate purposes with candidate consent and only by authorised employees of our agency.

Participation of Individuals/Complaints

- Candidates are entitled access to, and to correct any information held by us.
- Complaints should be submitted in writing to the Information Officer for Resolution.
- Requests to Access, Correct or Delete information must be made and submitted in writing to the Information Officer.

Operational Considerations –

Monitoring

The Management and Information Officer are responsible for ensuring adherence to Standard Operating Procedures.
All employees directly associated with recruiting activities will be trained in the regulatory requirements governing the protection of Personal Information.
We will conduct periodic reviews and training, where appropriate, to ensure compliance with this policy and guidelines.

Policy Compliance

Any breach of this policy could result in disciplinary action.

Policy on dealing with a Data Breach

Where there are reasonable grounds to believe that personal information under our control has been accessed or acquired by any unauthorised person, we will notify—

1. the Regulator; and
2. the candidate/client concerned.

The notification will be made as soon as reasonably possible after discovery of the breach taking into account the needs of law enforcement as well as measures necessary to determine the scope of the breach and to restore the integrity of the information system.

The notification to a Candidate must be in writing and communicated in at least one of the following ways:

1. By mail to the last known physical or postal address;
2. By e-mail to the last known e-mail address;
3. By posting in a prominent position on your website;
4. As may be directed by the Regulator.

The notification will provide sufficient information to allow the candidate/client to take protective measures against the potential consequences of the breach.