PROTECTION OF PERSONAL INFORMATION ACT POLICY

Key Recruitment

PostNet Suite #151, Private Bag X26, Tokai 7966

Phone number: +27 21 531-2015

Email address Information Officer: Justin@keyrecruitment.co.za

Introduction

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

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.

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

The **Information Officer**, (Justin Durandt), is responsible for:

- The monitoring of this policy;
- Ensuring that this policy is supported by appropriate documentation;
- Ensuring that this policy and subsequent updates are communicated to relevant managers, representatives, staff and associates, 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 must satisfy 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 only 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.

Specific Purpose

- Personal information collected from candidates will be used to secure Permanent or Temporary employment on behalf of Candidates.

Limitation on Further Processing

- Personal information may not be further processed in a way that is incompatible with the initial purpose for which it was collected and will only be done with the express consent of the Candidate

Information Quality

- We shall ensure that candidate information is complete, up to date and accurate before we use it. We will request candidates, at least once annually, to update their information and confirm that we may continue to store/retain same. If we are unable to contact a candidate their information will be deleted from our records.

Transparency/Openness

- Where personal information is collected from a source other than directly from a candidate (EG Social media, Job portals) we will make candidates aware:
    - That their information is being collected and the specific reason;
    - Who is collecting their information by giving them our details;

Data Security Safeguards

- 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 on the attached *Annexures 1 and 2* and submitted to the Information Officer.

Operational Considerations

Monitoring

The Board/Management and Information Officer are responsible for ensuring adherence to Standard Operating Procedures.

All employees and individuals directly associated with recruiting activities will be trained in the regulatory requirements governing the protection of Personal Information.

We will conduct periodic reviews and audits, where appropriate, to ensure compliance with this policy and guidelines.

Policy Compliance

Breach/es of this policy could result in disciplinary action and termination of employment.

ooOOoo

Annexure 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018 [Regulation 2]

Notes:

1. Affidavits or other documentary evidence in support of the objection may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Complete as is applicable.

DETAILS OF DATA SUBJECT

Name(s) and surname of data subject:
Unique Identifier/ Identity Number
Residential, postal or business address:
Contact number(s):
E-mail address:

DETAILS OF RESPONSIBLE PARTY

Name /Registered name of responsible party:
Residential, postal or business address:
Contact number(s):
E-mail address:

REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f)

Please provide detailed reasons for the objection below:

Signed at ..... this ..... day of .....20……..

.....
Signature of data subject/designated person

Annexure 2

REQUEST FOR ACCESS TO/CORRECTION/DELETION OF PERSONAL INFORMATION OR DESTROYING/DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE POPI ACT, 2013 (ACT NO. 4 OF 2013) REGULATIONS, 2018 [Regulation 3]

Notes:

1. Affidavits or other documentary evidence in support of the objection may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Complete as is applicable.

Mark the appropriate request box with an X

☐ Access to/Correction or deletion of personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

DETAILS OF DATA SUBJECT

Name(s) and surname of data subject:
Unique Identifier/ Identity Number:
Residential, postal or business address:
Contact number(s):
E-mail address:

DETAILS OF RESPONSIBLE PARTY

Name /Registered name of responsible party:
Residential, postal or business address:
Contact number(s):
E-mail address:

INFORMATION TO BE ACCESSED/CORRECTED/DELETED/DESTROYED (Circle applicable request)

Give description of Information:

Give detailed reasons for the request:

Signed at ..... this ..... day of .....20……..

.....
Signature of data subject/ designated person