PROTECTION OF PERSONAL INFORMATION

POLICY MANUAL
AND
COMPLIANCE FRAMEWORK

Table of Contents

1. Company Details 2
2. Introduction 2
3. Policy Principles 3
Principle 1: Accountability 3
Principle 2: Processing Limitation 3
Principle 3: Specific Purpose 3
Principle 4: Limitation on Further Processing 4
Principle 5: Information Quality 4
Principle 6: Transparency/Openness 4
Principle 7: Security Safeguards 4
Principle 8: Participation of Individuals 4
4. Operational Considerations 5
Monitoring 5
Operating controls 5
Policy Compliance 5

1. Company Details

AFFIRMATIVE PORTFOLIOS (PTY) LTD

Affirmative Portfolios Recruitment Consultants is a generalist Recruitment and HR Services Company. We provide a professional recruitment service to companies across a broad spectrum of disciplines. Our several branches including Durban, Bryanston, Cape Town, Pietermaritzburg and Port Elizabeth are able to assist

With: -

Temporary Employment Services, Permanent Staffing Solutions, Probation Management, Response Handling, Independent Payroll Solutions and Verification Checks.

Information Officer Details

Physical Address:
1st Floor
6 Pencarrow Park
La Lucia Ridge Office Estate

Postal Address:
P.O. Box 5017
Pencarrow Park
4019

Tel: +27 (0) 31 566 6474

Fax: +27 (0) 31 566 6493

Contact: Neil Bell

Email: durban@affirm.co.za

Website: www.affirmativeportfolios.co.za

2. Introduction

We are committed to compliance with The Protection of Personal Information (POPI) Act which 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, (Neil Bell), 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 relevant managers, representatives, staff and associates, where applicable.

All employees, subsidiaries, business units, departments and individuals directly associated with us are responsible for adhering to this policy and for reporting any security breaches or incidents to the Information Officer.

Any Service Provider that provides Information Technology services, including data storage facilities, to our organisation must adhere to the requirements of the POPI Act to ensure Adequate protection of personal information held by them on our behalf. Written confirmation to this effect must be obtained from relevant service providers.

3. 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, 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 (EG Social media, portals) 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.

4. Operational Considerations

Monitoring

The Management and Information Officer are 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. All employees, subsidiaries, business units, departments and individuals directly associated with us are to be trained, according to their functions, in the regulatory requirements, policies and guidelines that govern the protection of personal information. 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.
- Incident reporting and management.
- User ID addition or removal.
- Information security training and education.
- Data backup.

Policy Compliance

Any breach/es of this policy may result in disciplinary action and possible termination of employment.