

POPI POLICY

1. DEFINITIONS

POPIA

Protection of Personal Information Act

Data Subject

Person to whom the personal information relates [natural or juristic person]

Responsible Person

The person who determines the purpose of and means for processing personal information

Operator

Person who processes personal information for a responsible person into a contract/mandate, without coming under direct authority of that party

Processing

Anything that you can do with personal information including collection, storage, modification, destruction, etc.

2. INTRODUCTION

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

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

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

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

Head Office: East London

Physical Address: 8 Suffolk Road, Berea
East London, 5241

Contact Number: 043 721 2299
Fax Number: 043 726 0396



Port Elizabeth Branch:

Contact Number: 041 450 5600
Fax Number: 086 292 7796

The **Information Officer**, Michelle Labuschagne, 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 organization must satisfy us that they provide adequate protection of data held by them on our behalf.

3. POLICY PRINCIPLES

Accountability for Data to be collected

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

Processing Limitation/Purpose for Data Collection

- We will collect personal information directly from Candidates/Clients.
- Personal Information from Social Networks and Job-seeker portals will be collected with the express consent of the Candidate/s.
- Once in our possession, we will only process or further process Candidate/Client information with their consent, except where we are required to do so by law. In the latter case, we will always inform the Candidate/Client.

Specific Purpose

- Personal information collected from Candidates/Clients will be used to secure Permanent or Temporary employment on behalf of Candidates, or for the purposes of training initiatives.

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/Client.

Information Quality

- We shall ensure that Candidate information is complete, up to date, and accurate before we use it. We request that all Candidates, at least once annually, 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: (a) That their information is being collected and the specific reason; (b) 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 database;
 - by a Data Storage Service Provider;
 - in any electronic devices (that will be Password protected).
- We are committed to ensuring that information is only used for legitimate purposes with Candidate/Client consent and only by authorized employees of our agency.

Participation of Individuals/Complaints

- Candidates/Clients are entitled to access and 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 Form C and submitted to the Information Officer.

4. OPERATIONAL CONSIDERATIONS

Monitoring

- Management and the Information Officer are responsible for ensuring adherence to Standard Operating Procedures.
- All employees and individuals directly associated with business 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.

5. ACCEPTABLE CHANNELS OF FORWARDING PERSONAL INFORMATION

- We wish to provide our Candidates with a better service and have implemented an online Candidate Registration portal to facilitate this goal.
- This secure online platform allows our Candidates to create their CV Profile, upload supporting documentation and update their CV when necessary.
- Your information is completely confidential, and only available to Abantu Staffing Solutions Consultants based at both our EL and PE branches.
- Candidates are able to access this platform via our website and logging in requires the Candidate to create their own confidential unique Username and Password. (please click on the website link below).

6. EXAMPLES OF DATA SUBJECTS

- Candidates
- Temporary employees
- Clients
- Abantu Staffing Solutions (Pty) Ltd. employees

7. EXAMPLES OF PERSONAL INFORMATION

Includes but not limited to:

- Identity or passport number
- Date of birth and age
- Phone numbers
- Email address
- Physical address
- Gender, race and ethnic origin
- Disability
- Biometric data
- Marital relationship status
- Criminal record
- Private correspondence
- Employment history and salary
- Financial information
- Educational information
- Physical and mental health information

8. DIRECT MARKETING

The following provisions will apply with regards to direct marketing campaigns:

- Existing Clients – may market similar products and services.
- New Clients – obtain consent first.
- May only request consent once.
- Opt-in and Opt-out provisions must be in place.
- Opt-out opportunities must be provided when information is first collected and with each subsequent communication.

9. STORAGE

- Personal information collected is to be stored digitally via our secure CRM system, DittoHire.
- Printing of documentation containing personal information is only to be done when absolutely necessary.
- Physical documentation containing personal information is to be filed immediately with restricted access.

10. DESTRUCTION OF PERSONAL INFORMATION

- Abantu Staffing Solutions (Pty) Ltd. will destroy all documentation containing personal information as needed.

Head Office: East London

Physical Address: 8 Suffolk Road, Berea
East London, 5241

Contact Number: 043 721 2299

Fax Number: 043 726 0396



Port Elizabeth Branch:

Contact Number: 041 450 5600

Fax Number: 086 292 7796

11. BREACH OF SOP

Step 1

- Inform One Level Up and Information Officer immediately.
- Secure personal information on the same day.

Step 2

- Complete an internal investigation within 24 hours and compile a report.

Step 3

- Inform Information Regulator as soon as possible.
- Inform Data Subject and Client where applicable.

Step 4

- Take corrective action to strengthen protocols and prevent future breaches.