

Data Protection Policy:

1. Introduction:

- Introduction to the data protection policy, explaining its purpose and importance.
- Statement of commitment to protecting candidate data in compliance with South African data protection laws, including the Protection of Personal Information Act (POPIA).

2. Scope:

- Explanation of the scope of the policy, including the types of candidate data covered and the processes involved in handling this data.

3. Principles of Data Protection:

- Statement of the key principles governing the handling of candidate data, such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.

4. Types of Candidate Data Collected:

- Description of the types of candidate data collected by the recruitment agency, including personal details, contact information, employment history, education, skills, and any other relevant information.

5. Purpose of Data Collection:

- Explanation of the purposes for which candidate data is collected, including matching candidates with job opportunities, assessing suitability for roles, and facilitating communication between candidates and clients.

6. Legal Basis for Processing:

- Identification of the legal bases for processing candidate data, such as consent, contractual necessity, legitimate interests, or compliance with legal obligations.

7. Data Collection and Consent:

- Explanation of how candidate data is collected, including through online forms, CV submissions, or third-party sources.
- Procedures for obtaining and documenting candidate consent for the collection, processing, and sharing of their data.

8. **Data Use and Sharing:**

- Guidelines for the use of candidate data by the recruitment agency, including restrictions on unauthorized access, disclosure, or sharing with third parties.
- Procedures for sharing candidate data with clients, including obtaining candidate consent where necessary.

9. **Data Retention:**

- Explanation of the retention periods for candidate data, including criteria for determining retention periods and procedures for securely deleting or anonymizing data when no longer needed.

10. **Data Security:**

- Description of the security measures in place to protect candidate data from unauthorized access, disclosure, alteration, or destruction, including physical, technical, and organizational safeguards.

11. **Data Subject Rights:**

- Explanation of the rights candidates have regarding their personal data, including the right to access, rectify, erase, restrict processing, data portability, and object to processing.
- Procedures for handling data subject requests and inquiries in accordance with POPIA requirements.

12. **Data Breach Response:**

- Procedures for detecting, assessing, and responding to data breaches involving candidate data, including notification requirements under POPIA.

13. **Training and Awareness:**

- Measures for raising awareness among staff members about data protection responsibilities and providing training on data protection policies and procedures.

14. **Policy Review and Updates:**

- Schedule for reviewing and updating the data protection policy to ensure ongoing compliance with legal requirements and changes in business practices.