Protection of Personal Information Policy

For ALL Staff

Policy stipulating the way to process personal information of employees and clients.

Date Compiled:

1 May 2021

Compiled by :

Ian Putter

Document ID:

BM – HR – P051

Date Approved: June 2021

_____

General Manager

CONTENTS

1 PURPOSE

1.1 To give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at—

1.1.1 balancing the right to privacy against other rights, particularly the right of access to information; and protecting important interests, including the free flow of information within the Republic and across international borders;

1.1.2 regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;

1.1.3 provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act.

2 SCOPE

2.1 This policy applies to Management or key individuals, representatives or staff of Botselo. Management is ultimately responsible for ensuring that information security is properly managed and to ensure that all staff, representatives and key individuals adhere to this policy.

2.2 External service providers such as labour, time and attendance, payroll software consultants, as well as suppliers to the company in general, must adhere to the same information security as Botselo and will confirm in a separate agreement that they have such security measures in place in respect of the processing personal information.

3 POLICY STATEMENT

3.1 Botselo recognizes that its first priority under the POPI Act is to avoid causing harm to individuals. In the main this means:

3.1.1 keeping information securely in the right hands, and

3.1.2 retention of good quality information. Secondly, Botselo aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account.

3.2 In addition to being open and transparent, Botselo will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

4 WHAT IS PERSONAL INFORMATION ?

4.1 Personal information'' means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, living juristic person, including, but not limited to—

4.1.1 Contact information – telephone number, email address, physical address, location and online ID.

4.1.2 Private correspondence.

4.1.3 Biometric information – physical or psychological behavioural characterization, blood type and fingerprints.

4.1.4 Demographic information – age, gender, race, date of birth, ethnicity, sexual orientation, religion and culture.

4.1.5 Opinions of and about a person or group.

4.1.6 History – employment, financial information, medical history, criminal history as well as educational history.

5 POLICY

5.1 *Engagement (advertising, recruitment and selection)*

5.1.1 The personal information of candidates will be obtained directly from them, or a recruitment agency, unless derived from a public platform.

5.1.2 Where a recruitment agency is used the applicant must give consent that his/her personal information be obtained from the agency.

5.1.3 The personal information of unsuccessful candidates will be destroyed once a decision has been taken not to employ them.

5.1.4 Examples of personal information in the engagement process are the following:

- Curriculum vitae
- Identity document
- Educational qualifications
- Interview information
- Psychometric test results where applicable
- E-mail address
- Cell phone number
- Criminal and background checks

5.2 *Onboarding process, including induction*

5.2.1 The information pertaining to a next of kin will only be processed with the consent of the specific person, as it is information related to an identifiable, living natural person.

5.2.2 The appointee must submit proof of the consent from the next of kin that his/her personal information can be processed.

5.2.3 Examples of personal information in the onboarding process are the following:

- Contract of employment
- Biographical information
- Next of kin contact details

- Medical aid information
- Bank details
- E-mail address
- Cell phone number
- Payslips
- SARS tax records

5.3 *Debtors administration*

5.3.1 In the process of credit applications the personal information of clients will be obtained directly from them and dealt with according to the applicable processing principles.

5.3.2 Examples of personal information in the credit application process are the following:

- Company registration documents
- Identity documents of directors
- Vat registration documents
- Annual financial statements
- Bank details
- Business and physical addresses of directors
- Trade references

5.4 *Day-to-day management*

5.4.1 The Employer will conduct ongoing analysis of personal information to verify the quality, accuracy and competencies of the personal information.

5.4.2 The Employer will conduct risk assessments to determine loopholes in the protection of personal information.

5.4.3 The Employer will revise and update HR policies and contractual arrangements.

5.4.4 The Employer will revise and update client information.

5.4.5 Examples of personal information in the day-to-day management process are the following

- Employee personal file
- Disciplinary records
- Leave applications
- Doctors' notes
- Screening records regarding Covid-19
- Drug and alcohol test results
- Performance reviews
- Information related to trade union membership

5.5 ***Termination***

5.5.1 The Employer will, save for the information that must be retained in terms of applicable legislation, dispose of information where an employee's employment is terminated.

5.5.2 Personal information retained for further processing in terms of section 15(e) of the Act, namely any contractual rights and obligations between the parties, will be processed solely for that purpose and will not be published in an identifiable form.

6 PRINCIPLES

6.1 ***Principle 1: Accountability***

6.1.1 Botselo will take reasonable steps to ensure that personal information obtained from the engagement process and onboarding process are stored safely and securely. This includes CV's, Resumes, References, Qualifications, Integrity Checks, on boarding documents and any other personal information that may be obtained for the purpose of onboarding and employment equity.

6.2 ***Principle 2: Processing Limitation***

6.2.1 Botselo will collect personal information directly from candidates/employee. Once in our possession we will only process or release candidate/employee information with their consent, except where we are required to do so by law. In the latter case we will always inform the candidate/employee.

6.3 ***Principle 3: Specific Purpose***

6.3.1 Botselo collect personal information from candidates/employees to enable us to process payroll and comply with legislation.

6.4 ***Principle 4: Limitation on Further Processing***

6.4.1 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 engagement, onboarding, terminations and by law requirements and it will only be used for that purpose.

6.5 ***Principle 5: Information Quality***

6.5.1 Botselo is 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.

6.6 ***Principle 6: Transparency/Openness***

6.6.1 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.

6.7 *Principle 7: Security Safeguards*

6.7.1 Botselo 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/employee consent and only by authorized employees of our company.

6.8 *Principle 8: Participation of Individuals*

6.8.1 Candidates/employees 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.

7 OPERATIONAL CONSIDERATIONS

7.1 *Monitoring*

7.1.1 The Board/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.

7.1.2 All employees, subsidiaries, business units, departments and individuals directly associated with Botselo are to be trained, according to their functions, in the regulatory requirements, policies and guidelines that govern the protection of personal information.

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

7.2 *Operating controls*

7.2.1 Botselo shall establish appropriate privacy standard operating controls 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.

8 IMPLEMENTATION AND COMPLIANCE

8.1 This policy will be adhered to by all key individuals, representatives and staff who are tasked with collecting and processing of personal information. Non-compliance with this policy may result in disciplinary action and possible termination of employment or mandate, where applicable.

9 COMPLAINTS PROCEDURE

9.1 Any complaint received regarding a breach of this policy will be dealt within the context of the prescriptions of the POPI Act.

9.2 The Employer's Information Officer (IO) will upon receiving the written complaint and supporting documentation log the date and contents of the complaint in the Complaints Register. The information about complaints must be kept for a period of five years.

9.3 The IO will lead the investigation with regard to the complaint, facilitate a session to find a solution and implement corrective actions, and to submit a report about the incident and outcomes within 30 days.

9.4 If unable to resolve the complaint within 30 days the IO will notify the complainant, giving full written reasons as to why the outcome was not favorable, and advise the complainant of their right to seek legal redress by referring the complaint to the Information Regulator.

9.5 The IO will update the Complaints Register with all developments and activities regarding complaints received.

We shall only collect, use, and keep personal information (either directly or through our service providers) if there is a lawful purpose for doing so.