Data Protection Policy

Version	2.3
Last updated	January 2025
Owner	Carol Peacock, Human Capital
Reviewer	BEE123 Legal (powered by Michalsons Giles Inc.)
Approver	Claudia Pather, Head of Operations
Implementation date	13 December 2024
Next revision date	January 2026
Other relevant policies	Privacy Policy, Data Retention and Disposal Policy, and Security and Incident Response Policy.

1. Purpose

At BEE123, we respect people's privacy and we protect the personal information we process. We balance our need to process personal information for our activities with the legal requirements to protect it.

The objective of this policy is to safeguard personal information and ensure we comply with applicable data protection laws and regulations. This policy describes the principles governing our processing of personal information and which principles we expect our employee to uphold in processing personal information. It also records our compliance strategy regarding personal information.

2. Scope

This policy applies to you if you are our employee. It governs all personal information we and our employee process in the course of our business.

3. Interpretation

In this policy,

- **account number** has the meaning given to it in section 105 of POPIA.[1] Essentially, it is a unique identifier that has been assigned to one or more data subjects by a financial or other institution which enables them to access their own funds or credit facilities. You may refer to section 1 in POPIA for the definition of "unique identifier";
- **children's personal information** refers to the personal information of a person under the age of 18;
- **data subject** means the person to whom personal information relates;
- **operator** has the meaning given to is under POPIA and is known as a "processor" under other data protection regulations. We are the operator when we process on behalf of another party in terms of a written agreement. For example, processing our clients' personal information to help them calculate their scorecards;
- **person** means a natural or juristic person;
- **personal information** has the meaning given to it under POPIA and is known as "personal data" under other data protection regulations.[2] Essentially, it is any information that: identifies a person, can be used or manipulated by a reasonably foreseeable method to identify the person; or can be linked by a reasonably foreseeable method to other information that identifies a person.
- **employee** or **you** include employees, management, directors, contractors, student learners, apprentices, interns, or volunteers; and
- **POPIA** refers to the Protection of Personal Information Act 4 of 2013 and the Regulations relating to the Protection of Personal Information Act;
- **processing** has the meaning given to it under POPIA. Essentially, it is anything you do with personal information. This includes collecting, storing, using, sharing, or deleting it, whether or not you use automatic means. For example,

[1] https://popia.co.za/section-105-unlawful-acts-by-responsible-party-in-connection-with-account-number/.
[2] https://popia.co.za/section-1-definitions/.

collecting information by reading a hard copy CV, storing it in your filing cabinet, using it in the interview process, and then shredding it after a certain period, you've processed personal information;

- **responsible party** has the meaning given to is under POPIA and is known as a "controller" under other data protection regulations. We are the responsible party when we determine the purpose of and means for processing personal information. For example, processing our employee's personal information for payroll;
- **special personal information** has the meaning given to it under POPIA and is known as "sensitive personal information". Essentially, it is personal information which, due to its sensitive nature, may result in greater harm to the data subject if it was processed unlawfully.
- **we**, **us**, **our**, or **BEE123** means BEE123 (Pty) Ltd (Registration number: 2016/150254/07) and its subsidiaries and affiliates.

4. Data Protection Laws

We are committed to protecting and respecting the privacy of our data subjects in accordance with the data protection law applicable to the jurisdiction in which we operate. The relevant data laws with which we will comply are:

- Protection of Personal Information Act 4 Of 2013; and
- Promotion of Access to Information Act of 2002.

While other jurisdictions' data protection laws do not apply to our processing, we will look to them for guidance where local data laws are silent on certain issues. In particular, we will consider the General Data Protection Regulation 2016/679 (European Union).

5. Data protection requirements

5.1. In applying the relevant data protection laws, you must help us ensure that we:

- enable data subject **rights**;
- adhere to our data protection **obligations** as responsible party or operator; and
- apply the data protection **principles**.

5.2. In terms of data subject **rights**, you must help us ensure that our data subjects can:

- **know** when and why we process their personal information;
- request **access** to their personal information that we process;
- **correct** any personal information of theirs that is incorrect;
- **erase** their personal information from our systems, where required;
- **restrict** our processing of their personal information, where required;
- **object** to our processing of their personal information; and
- be protected from us making **automated decisions** about them.

5.3. In terms of our **obligations as responsible party**, you must help us ensure that we:

- implement appropriate and reasonable technical and organisational **measures** to protect personal information;
- control our operators through a written **contract**;
- keep **records** of our processing activities;
- **co-operate** with the relevant data protection authorities;
- conduct data protection impact **assessments**, where required;
- **consult** with the relevant data protection authorities, where required;

5.4. In terms of our obligations as operator, you must help us ensure we:

- enter into a **contract** with the relevant responsible party;
- process personal information only on the **instructions** of the responsible party;
- keep **records** of our processing activities done on behalf of the responsible party;
- inform the relevant data protection authorities of **irregularities**, where required;

5.5. In terms of the data protection **principles**, we will ensure that we process and you must ensure that you process personal information:

- **lawfully**, fairly and transparently;
- only for a **specific purpose** that is explicit and legitimate;

- only **as necessary** for that purpose;
- **accurately**, and is kept up to date;
- for **no longer** than necessary to achieve the purpose; and
- **securely**.

6. Codes and standards

In terms of our processing activities, we take guidance from ISO 27001 (information security management).

7. Compliance strategy

This policy sets out our compliance strategy for data protection specifically. Our compliance strategy is to do what is reasonably practicable to comply with those aspects of data protection that apply to our business, under the applicable data protection law. We will enable data subject rights and adhere to our relevant obligations. We have adopted a risk-based approach to applying the data protection principles. We seek to maintain a balance between what is required by law and what is practical in our specific circumstances. We are committed to achieving **absolute compliance** and will do our best to comply absolutely with every aspect of the applicable data protection law.

We have identified the following areas as being key priorities in our compliance efforts:

- **monitoring and applying** our data protection activities consistently across our business;
- adopting **privacy by design** and by default at a companywide level;
- managing our **operator relationships** efficiently; and
- **digitising** our data processing activities.

8. Roles and responsibilities

8.1. Employee

8.1.1. All employee must,

- comply with this policy and those policies and procedures related to it;
- participate in and complete data protection training and awareness initiatives;
- comply with the data protection principles in processing personal information;
- ensure that any form of direct marketing provides the data subject with the opportunity to opt out of future direct marketing;
- take particular care when processing children's personal information, special personal information, or account numbers; and
- report any data incident to your line manager as quickly as possible and in accordance with the Security and Incident Response Policy.

8.1.2. Please note that section 20 of POPIA applies to you as our employee. It applies to our operators and includes our employees. It states that you must,

- only process personal information with our knowledge or authorisation;
- treat personal information which comes to your knowledge as confidential; and
- you must not disclose it, unless required in the proper performance of your duties or by law.

8.2. Information Officer

8.2.1. **Governance of data protection.** We have appointed an Information Officer. The Information Officer is responsible for the governance of data protection. We will appoint and maintain one Information Officer for all of our entities.

8.2.2. **Responsibilities.** The Information Officer is responsible for:

- **promoting compliance** with data protection law within the entity;
- **ensuring awareness** of data protection law within the entity;
- managing and responding to data subject **access requests**;
- managing and responding to data **breaches or incidents**;
- assisting the relevant data protection authority **investigations**;
- developing, implementing and monitoring the **compliance framework** within the entity; and
- ensuring that **this policy** is useful and relevant.

8.2.3. The Information Officer will report to the CEO.

8.2.4. The Information Officer is the entity's compliance function for the purposes of data protection compliance. Their contact information is:

Name	Email	Phone
Claudia Pather	Claudia.Pather@bee123.co.za	+27 82 386 4719

9. Consequences for violation

Any breach of this policy may result in appropriate disciplinary action related to the severity of a employee member's breach and their failure to comply with their obligations under this policy.

10. Changes

We may change the terms of this policy at any time and where this affects your rights and obligations, we will notify you of any changes by email.

11. Reviewing and updating this policy

This policy and its annexures will be reviewed on at least an annual basis. The details of the current version and next review appear on the cover page. The information below provides a description of the update made in a review.

Date	Version	By whom	Description of update
10/04/2024	V2.2	Edunne Patz	
09/12/2024	V2.3	BEE123 Legal (powered by Michalsons Giles Inc.)	• Updated to plain legal language to improve readability and understanding of employee obligations. • Removed the parts of the policy that restated the obligations set out in the Act, which BEE123 must comply with regardless of their inclusion or statement in the policy. The Act sets out principles which an organisation must adhere to and are not suitably targeted to the employee of such organisation. • Clarified expectations of employee members and the Information Officer's role in driving data governance.

12. APPROVAL AND ADOPTION

This policy has been approved and adopted by the following authorised BEE123 representatives:

CPather

Signature
Name : Claudia Pather
Role: Head of Operations

22-01-2025

Date : 22 January 2025

Signature
Name: Carol Peacock
Role: Human Resources

22/01/2025

Date 22 January 2025