CHRIS BAKER & ASSOCIATES

INCORPORATED

POPI Policy



Chris Baker & Associates

ATTORNEYS

Table of Contents

1. Introduction

2. Definitions

3. Policy Purpose

4. Scope and Application

5. Rights of Data Subjects

6. General Guiding Principles

7. Information Officer

8. Specific Duties and Responsibilities

9. Processing of Personal Information

10. Information Security Measures

11. Data Subject Access Requests

12. POPI Complaints Procedure

13. Disciplinary Action

14. Amendments to this Policy

1. Introduction

Chris Baker & Associates Incorporated (CBA) is committed to protecting the privacy and security of personal information of our employees, clients, suppliers, and other stakeholders. This policy outlines our approach to compliance with the Protection of Personal Information Act 4 of 2013 (POPIA), the Promotion of Access to Information Act 2 of 2000 (PAIA), the Electronic Communications and Transactions Act 25 of 2002, the Cybercrimes Act 19 of 2020, applicable labour legislation, professional confidentiality obligations, applicable rules of the Legal Practice Council, and any guidance notes, notices, regulations, codes of conduct or enforcement notices issued by the Information Regulator from time to time.

The right to privacy is an integral human right recognized and protected in the South African Constitution. POPIA aims to give effect to this constitutional right by safeguarding personal information when processed by a responsible party. CBA acknowledges its obligation to comply with the provisions of POPIA and to ensure that personal information is processed lawfully and transparently.

2. Definitions

For the purposes of this policy, the following definitions apply:

- **"Personal Information"** means information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person.
- **"Data Subject"** means the person to whom personal information relates.
- **"Responsible Party"** means CBA, as the entity which determines the purpose of and means for processing personal information.
- **"Operator"** means a person who processes personal information for CBA in terms of a contract or mandate, without coming under the direct authority of CBA.
- **"Processing"** means any operation or activity concerning personal information, including collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as restriction, degradation, erasure or destruction of information.
- **"Record"** means any recorded information regardless of form or medium.
- **"Information Officer"** means the person responsible for ensuring CBA's compliance with POPIA.
- **"Special Personal Information"** means personal information concerning, among other things, a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, or criminal behaviour, as contemplated in POPIA.
- **"Child"** means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning that person.
- **"Consent"** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

3. Policy Purpose

The purpose of this policy, which is to be read along with the PAIA Manual as it sheds additional light on these matters, is to:

a) Comply with the provisions of POPIA and establish the requirements for the lawful processing of

personal information.

b) Protect CBA from the compliance risks associated with the protection of personal information.

c) Outline the principles which are binding on CBA and all its employees and contractors with regard to the processing of personal information.

d) Create awareness about the importance of privacy and data protection among CBA stakeholders.

e) Provide guidelines for the collection, use, storage and disclosure of personal information.

4. Scope and Application

This policy applies to:

a) The board of directors, management, and all employees of CBA.

b) All clients, contractors, suppliers, and other persons acting on behalf of CBA.

c) All CBA's operations, business units, and divisions.

d) All personal information processed by CBA, in both electronic and physical format.

The policy must be read in conjunction with other relevant CBA policies and procedures, including the Privacy Policy.

5. Rights of Data Subjects

CBA recognizes and respects the rights of data subjects. These rights include:

a) The right to be notified that personal information is being collected or has been accessed by unauthorized persons.

b) The right to establish whether CBA holds personal information and to request access to such information.

c) The right to request correction, destruction, or deletion of personal information.

d) The right to object to the processing of personal information.

e) The right not to have personal information processed for the purposes of direct marketing by means of unsolicited electronic communications.

f) The right to submit a complaint to the Information Regulator regarding alleged interference with protection of personal information.

g) The right to institute civil proceedings regarding alleged interference with the protection of personal information.

CBA will ensure that these rights are respected and upheld in all its operations.

6. General Guiding Principles

CBA is committed to processing personal information lawfully and implementing appropriate safeguards. The following principles guide our approach:

6.1 Accountability

CBA takes responsibility for complying with POPIA and implementing measures to demonstrate compliance.

6.2 Processing Limitation

Personal information is processed lawfully, reasonably, and in a manner that does not infringe on the privacy of the data subject.

6.3 Purpose Specification

Personal information is collected for specific, explicitly defined, and lawful purposes.

6.4 Further Processing Limitation

Further processing of personal information must be compatible with the purpose for which it was initially collected.

6.5 Information Quality

Reasonable steps are taken to ensure personal information is complete, accurate, not misleading, and updated where necessary.

6.6 Openness

Data subjects are informed about the collection and processing of their personal information.

6.7 Security Safeguards

The integrity and confidentiality of personal information is secured through appropriate technical and organizational measures.

6.8 Data Subject Participation

a) Data subjects have the right to participate in the processing of their personal information by requesting confirmation of whether CBA holds personal information about them, requesting access to such personal information, and requesting the correction, deletion or destruction of personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, unlawfully obtained or no longer authorised to be retained.

b) Requests relating to access to records must be dealt with in accordance with POPIA, PAIA, the PAIA Regulations, CBA's PAIA Manual, the prescribed request forms, applicable fees, prescribed time periods, lawful grounds for refusal, confidentiality obligations, legal privilege and any applicable complaint or court processes.

c) CBA will document and process such requests through the Information Officer or Deputy Information Officer, verify the requester's identity and authority where required, consider the lawful basis and purpose for the relevant processing activity, and maintain appropriate internal records of the request, decision, outcome and any corrective action taken.

7. Information Officer

CBA has appointed an Information Officer who is responsible for:

a) Encouraging and ensuring compliance with POPIA.

b) Developing, publishing, and maintaining this POPI Policy.

c) Handling data subject access requests.

d) Working with the Information Regulator in relation to investigations.

e) Ensuring that appropriate processes and controls are implemented for the protection of personal information.

f) Overseeing the processing of personal information by CBA.

The contact details of the Information Officer are:

Sara Amy Blumberg, Director, sara@cbalaw.biz, 071 885 9863.

8. Specific Duties and Responsibilities

8.1 Executive Directors

The Executive Directors are ultimately accountable for ensuring that CBA meets its legal obligations in terms of POPIA. They are responsible for:

a) Approving and overseeing this POPI Policy.

b) Ensuring adequate resources are allocated for POPIA compliance.

c) Reviewing POPIA compliance at least annually.

8.2 Management

Management is responsible for:

a) Ensuring that this POPI Policy is implemented within their areas of responsibility.

b) Supporting the Information Officer in performing their duties.

c) Ensuring staff are trained on POPIA requirements.

8.3 Employees

All employees are responsible for:

a) Familiarizing themselves with this POPI Policy and complying with its provisions.

b) Reporting any suspected or actual breaches of personal information to the Information Officer.

c) Only accessing and processing personal information where necessary for their job functions.

8.4 IT Department and Contractors

The IT Department and their Contractors are responsible for:

a) Implementing appropriate technical measures to protect personal information.

b) Assisting the Information Officer with data subject access requests.

c) Ensuring systems comply with POPIA requirements.

9. Processing of Personal Information

9.1 Purpose of Processing

9.1.1. CBA will only process personal information for specific, explicitly defined, lawful and legitimate purposes connected to its business, professional, employment, statutory, compliance and operational activities. These purposes include, where applicable:

a) providing services to clients
b) facilitating transactions with data subjects
c) fulfilling contractual obligations to clients and client contacts
d) administering employee and supplier relationships
e) complying with legislation and regulatory obligations
f) attending to legitimate interests
g) verifying identity and authority for security purposes
h) maintaining accounts and records
i) conducting audits and recordkeeping
j) conducting market or customer satisfaction research
k) improving services
l) supporting lawful sales and marketing activities
m) dealing with legal proceedings, and
n) engaging with business partners, operators, regulators, courts, tribunals, professional advisers and other recipients where POPIA, PAIA, another law, a contract, consent, legitimate interest or another lawful basis permits or requires such processing.

9.1.2. Before collecting personal information, CBA will take reasonably practicable steps to ensure that:

a) the data subject is aware of the personal information being collected
b) the source of the information if it is not collected directly from the data subject
c) the purpose of collection and processing
d) whether the supply of information is voluntary or mandatory
e) the consequences of failing to provide the information
f) any law authorising or requiring collection
g) the recipients or categories of recipients to whom the information may be supplied
h) any planned cross-border transfer or processing outside the Republic of South Africa, and
i) the data subject's rights under POPIA and PAIA, including the right to request access to, correction, deletion or destruction of personal information and the right to lodge a complaint with the Information Regulator or approach a competent court where applicable.

9.2 Categories of Data Subjects

CBA may process personal information relating to the following categories of data subjects:

a) Clients

b) Employees

c) Contractors and suppliers

d) Directors and shareholders

e) Job applicants

9.3 Types of Information

The types of information processed may include:

a) Contact details

b) Demographic information

c) Employment history

d) Financial information

e) Educational information

f) Medical information (where relevant)

g) Biometric information

h) criminal history information

i) health information

j) trade union information, and

k) other special personal information, but only where permitted by POPIA, another applicable law, the data subject's consent, or another recognised justification.

l) other information as may be legitimately required in the course and scope of running the business

9.4 Recipients of Personal Information

CBA may share personal information with recipients or categories of recipients where POPIA, PAIA, another applicable law, a contract, consent, legitimate interest or another lawful basis permits or requires such sharing. These recipients may include, where applicable:

a) service providers and operators
b) professional advisers
c) auditors
d) consultants
e) business partners
f) IT and cloud service providers
g) payroll and HR service providers
h) marketing and website service providers
i) banks and financial institutions
j) insurers
k) medical aid or employee benefit providers
l) regulators
m) courts
n) tribunals
o) government departments

p) law enforcement authorities
q) the Information Regulator
r) SARS
s) CIPC
t) the Department of Employment and Labour
u) the UIF
v) the Compensation Fund
w) the CCMA and/or Bargaining Councils
x) verification agencies and other third parties where necessary for CBA's business, professional, statutory, contractual, employment, legal, compliance or operational purposes.

CBA may also provide personal information to CBA's business partners, including Global Business Solutions, Kirchmanns Incorporated, Circle and Square, Joint Prosperity, Inscape Properties and/or contracted operators, where this is lawful and appropriate for business sustainability, client engagement, service delivery, lawful sales and marketing activities, or related purposes. Any sharing of personal information with business partners, operators or third parties will only take place where CBA has a lawful basis to do so, including consent, an existing client relationship, contractual necessity, legal obligation, legitimate interest, or another ground permitted by POPIA.

Where personal information is shared with operators or service providers, CBA must ensure that written agreements are in place requiring the operator or service provider to process personal information only with CBA's knowledge or authorisation, maintain confidentiality, implement appropriate security safeguards, notify CBA immediately of any actual or suspected compromise of personal information, assist CBA with data subject requests and regulatory obligations where applicable, and return, delete or securely destroy personal information when the services end, subject to lawful retention requirements.

Personal information may be transferred outside South Africa only where POPIA permits such transfer, including where the recipient is subject to a law, binding corporate rules or binding agreement providing an adequate level of protection, where the data subject consents, where the transfer is necessary for the performance of a contract or pre-contractual measures, or where another lawful ground applies. Cross-border transfers must be recorded in CBA's processing register or other appropriate internal compliance record.

Direct marketing by electronic communication may be conducted only in accordance with POPIA, including section 69. CBA must ensure that unsolicited electronic marketing is sent only where permitted, that consent is obtained where required, that every marketing communication identifies CBA as the sender, and that data subjects are given a clear and practical opportunity to opt out of further marketing communications.

10. Information Security Measures

CBA implements appropriate, reasonable technical and organisational measures to secure the integrity, confidentiality and availability of personal information and to prevent loss, damage, unauthorised access, unlawful access, unauthorised processing or unlawful processing of personal information.

These safeguards may include, where appropriate, role-based access controls, strong password and authentication controls, multi-factor authentication, encryption or secure transmission methods, secure backups, anti-virus and anti-malware protection, patch management, secure

configuration standards, clean-desk and clear-screen controls, physical security controls, secure disposal of paper and electronic records, incident logging, periodic access reviews, confidentiality undertakings, staff awareness training, operator and technology provider due diligence, and monitoring, investigation and response procedures for security incidents.

CBA will review its security controls and related processes on a regular basis to ensure that personal information remains secure and that safeguards remain appropriate to the nature of the information processed, the risks associated with the processing, the available technology, and the cost of implementation.

If there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, CBA must notify the Information Regulator and affected data subjects as soon as reasonably possible, unless a competent authority determines that notification will impede a criminal investigation. The notification should contain sufficient information to allow affected data subjects to take protective measures.

CBA must retain personal information only for as long as necessary to fulfil the purpose for which it was collected, unless retention is required or authorised by law, reasonably required for lawful purposes related to CBA's functions or activities, required by contract, or consented to by the data subject. Personal information that is no longer required must be securely destroyed, deleted or de-identified in a manner that prevents reconstruction in intelligible form.

11. Data Subject Access Requests

Data subjects have the right to request confirmation of whether CBA holds personal information about them and to request access to such personal information, subject to POPIA, PAIA, the PAIA Regulations, CBA's PAIA Manual, applicable confidentiality obligations, legal privilege, prescribed forms, applicable fees, prescribed time periods and lawful grounds for refusal.

Requests for access to records must be handled with reference to PAIA where applicable, including the prescribed PAIA request form, sufficient particulars to identify the record and requester, proof of authority where the request is made on behalf of another person, identification of the right to be exercised or protected where required by PAIA, applicable request and access fees, prescribed time periods, grounds for refusal, complaint mechanisms and court processes.

Requests for correction, deletion, destruction or objection to processing must be handled in accordance with POPIA and documented by the Information Officer or Deputy Information Officer. CBA will take reasonable steps to verify the requester's identity and authority, assess the request in accordance with POPIA and PAIA, communicate the outcome to the requester, and maintain appropriate internal records of the request, decision, outcome and any corrective action taken.

12. POPI Complaints Procedure

Data subjects may lodge a complaint with CBA's Information Officer or Deputy Information Officer regarding the processing of their personal information, an alleged interference with the protection of their personal information, or a concern relating to access, correction, deletion, destruction, objection, direct marketing, security safeguards or any other POPIA-related matter.

CBA will investigate complaints within a reasonable time, request further information where necessary, consider the complaint in accordance with POPIA, PAIA, the PAIA Manual and any applicable internal policies or procedures, and provide feedback to the complainant where

appropriate.

Complaints should be recorded in a complaints register stating the date received, complainant details, nature of the complaint, responsible person, investigation steps, outcome, remedial action and date finalised. Where appropriate, complainants should be informed that complaints may be submitted to the Information Regulator using the prescribed complaints process and contact details published by the Information Regulator.

If a complainant is dissatisfied with CBA's response, they may lodge a complaint with the Information Regulator and/or approach a competent court for appropriate relief, where applicable.

13. Disciplinary Action

Non-compliance with this policy, POPIA, PAIA, CBA's PAIA Manual, any applicable information security policy, confidentiality obligation, operator agreement, data protection procedure or lawful instruction relating to the protection of personal information may result in disciplinary action, contractual remedies, termination of employment or termination of the applicable business relationship, depending on the nature and seriousness of the non-compliance.

Certain breaches may also result in civil, criminal, regulatory or professional consequences, including reporting to the Information Regulator or another competent authority where required or appropriate. CBA will consider each matter on its own facts and will act in accordance with applicable labour law, contractual obligations, professional obligations and internal disciplinary procedures.

14. Amendments to this Policy

This policy should be formally reviewed at least annually and whenever there are material changes to POPIA, PAIA, Information Regulator guidance, CBA's PAIA Manual, CBA's processing activities, technology systems, operators, services, business partners, security risks, incident history, legal obligations or operational requirements.

The review should be documented, approved by management, and communicated to relevant staff and stakeholders where appropriate. CBA may amend this policy from time to time to ensure ongoing compliance with POPIA, PAIA and other relevant legislation, and to ensure that the policy remains aligned with CBA's business, professional, compliance and operational requirements.

Last updated: 7 October 2026

Approved by: Sara Amy Blumberg, Director