

23 June 2026

RE: PROTECTION OF PERSONAL INFORMATION POLICY (POPIA)

1. PURPOSE

- 1.1. The purpose of this Policy is to ensure that Bridgepoint Legal Consultants (Pty) Ltd (“Bridgepoint”) processes personal information lawfully, responsibly, and in accordance with the Protection of Personal Information Act (“POPIA”).
- 1.2. Bridgepoint is committed to protecting the privacy, confidentiality, and integrity of personal information entrusted to it by clients, employees, contractors, suppliers, and other stakeholders.

2. SCOPE

- 2.1. This Policy applies to:

- Directors
- Employees
- Contractors
- Consultants
- Temporary staff
- Service providers acting on behalf of Bridgepoint

The Policy applies to all personal information processed by Bridgepoint, whether in physical or electronic format.

3. DEFINITIONS

- 3.1. Data Subject:

- 3.1.1. The individual or juristic person whom the personal information relates to

- 3.2. Processing:

- 3.2.1. Any operation involving personal information including:
 - Collection
 - Storage

- Recording
- Updating
- Sharing
- Destruction

3.3. Personal information

3.3.1. Information relating to an identifiable living natural person or existing juristic person, including but not limited to:

- Names
- Identity numbers
- Contact details
- Employment information
- Financial information
- Correspondence
- Opinions and evaluations

4. PRINCIPLES OF PROCESSING

- 4.1. Accountability - Bridgepoint accepts responsibility for compliance with POPIA
- 4.2. Lawfulness - Information shall only be processed where there is a lawful basis
- 4.3. Specific Purpose – Information shall only be collected for a legitimate purpose
- 4.4. Limitations – Only information required for the intended purpose shall be collected
- 4.5. Accuracy – Reasonable steps shall be taken to ensure information is accurate and up to date
- 4.6. Security – Appropriate safeguards shall be implemented
- 4.7. Transparency – Data subjects shall be informed regarding the processing of their personal information

5. PERSONAL INFORMATION PROCESSED

5.1. Client Information

- Names
- Identity numbers
- Contact details
- Employment records
- Disciplinary documentation
- Arbitration records
- Financial information

5.2. Employee Information

- Personnel records
- Payroll records
- Medical certificates
- Performance records

6. **PURPOSES FOR PROCESSING**

6.1. Bridgepoint processes information for:

- Provision of legal consulting services
- Labour relations services
- Dispute resolution services
- Employment administration
- Payroll administration
- Compliance with legal obligations
- Financial management
- Marketing activities where permitted by law

7. **LAWFUL BASIS FOR PROCESSING**

7.1. Personal information may be processed where:

- Consent has been obtained;
- Processing is necessary to perform a contract;
- Processing is required by law;
- Processing protects a legitimate interest of the data subject;
- Processing protects Bridgepoint's legitimate business interests.

8. **DISCLOSURE OF PERSONAL INFORMATION**

8.1. Disclosure shall be limited to what is reasonably necessary.

8.2. Bridgepoint may disclose information to:

- Courts
- CCMA
- Bargaining Councils
- Government departments
- Professional advisors
- Auditors

- IT service providers
- External consultants
- SARS

9. INFORMATION SECURITY

9.1. Employees shall not share passwords or grant unauthorised access to company information.

9.2. Bridgepoint shall implement reasonable technical and organisational measures including:

- Password protection
- Multi-factor authentication
- Anti-virus protection
- Secure cloud storage
- Access controls
- Physical security measures
- Secure disposal of information

10. RETENTION OF INFORMATION

10.1. Personal information shall be retained only for as long as:

- Required by law;
- Required for business purposes;
- Necessary to resolve disputes.

Where information is no longer required, it shall be securely destroyed.

11. RIGHTS OF DATA SUBJECTS

11.1. Data subjects have the right to:

- Access their personal information;
- Request correction of information;
- Request deletion where legally permissible;
- Object to processing;
- Withdraw consent where processing is based on consent;
- Lodge complaints with the Information Regulator.

12. DATA BREACHES

12.1. Any employee who becomes aware of any data breach must report it to the information officer

12.2. Examples include but is not limited to:

- Lost devices;
- Incorrect emails sent to third parties;
- Unauthorised access;
- Hacking incidents;
- Disclosure of confidential information.

12.3. An investigation will be done in accordance with the company's procedures herein.

13. INFORMATION OFFICER

13.1. Stefan Pretorius (stefan@bridgepointlegal.co.za)

13.2. Responsible for:

- Monitoring POPIA compliance;
- Managing requests from data subjects;
- Conducting awareness training;
- Maintaining compliance documentation;
- Liaising with the Information Regulator.

14. EMPLOYEE RESPONSIBILITIES

14.1. Employees must:

- Protect confidential information;
- Follow security procedures;
- Report incidents immediately;
- Process information only for authorised purposes;
- Attend POPIA training where required.

Failure to comply may result in disciplinary action.

15. POLICY REVIEW

15.1. This Policy shall be reviewed annually or whenever legislative changes require amendment.

Signed and approved on this 23rd day of June 2026.



SL Pretorius

Director



M Swanepoel-Jooste

Director