POPIA Compliance Framework

[Creative Media Innovation (PTY) LTD] | CMI Bridge SaaS Platform

Effective Date: 7 May 2026 | Version: 1.0

This document sets out [Creative Media Innovation (PTY) LTD]'s ('Company') framework for compliance with the Protection of Personal Information Act 4 of 2013 ('POPIA'), which came into full effect on 1 July 2021. It describes how we collect, use, store, share, and protect personal information, and how we fulfil our obligations as a responsible party under POPIA.

Legal Context

POPIA is South Africa's primary data protection law. It gives effect to the constitutional right to privacy and regulates the processing of personal information by public and private bodies.

Non-compliance may result in enforcement action by the Information Regulator, administrative fines of up to R10 million, and/or imprisonment of up to 10 years for certain offences.

This framework applies to all personal information processed by the Company in connection with the Platform, whether collected from Customers, Users, employees, or third parties.

1. Key Definitions Under POPIA

The following terms have specific meanings under POPIA and are used throughout this document:

- Personal Information: Any information relating to an identifiable, living natural person (or juristic person), including names, contact details, ID numbers, financial information, biometric data, opinions, and online identifiers.
- Processing: Any operation performed on personal information, including collection, storage, use, dissemination, modification, or destruction.
- Responsible Party: The entity that determines the purpose and means of processing personal information. The Company is the responsible party for information it collects directly. For Customer Data, the Customer is the responsible party and the Company acts as an operator.
- Operator: An entity that processes personal information on behalf of a responsible party. The Company acts as an operator when processing Customer Data under instruction.
- Data Subject: The individual to whom the personal information relates.
- Special Personal Information: A category of sensitive data afforded extra protection, including religious beliefs, race, health, sexual orientation, criminal history, biometric data, and children's information.
- Information Officer: The person responsible for POPIA compliance within the Company, registered with the Information Regulator.
- Information Regulator: The South African regulatory body that enforces POPIA (inforeg@justice.gov.za).

2. Information Officer

In accordance with section 55 of POPIA, the Company has designated an Information Officer responsible for:

- Ensuring compliance with POPIA and this framework;
- Dealing with requests made by data subjects;
- Working with the Information Regulator on complaints and investigations;
- Developing, implementing, and monitoring a POPIA compliance programme;
- Conducting or overseeing Privacy Impact Assessments (PIAs).

Information Officer Contact Details:

Name: [Information Officer Name]

Email: privacy@[yourcompany].com

Address: [Your Business Address], South Africa

Registration Requirement

The Information Officer must be registered with the Information Regulator. Registration is completed at www.justice.gov.za/inforeg.

Deputy Information Officers may be designated for operational support and must also be registered.

3. The Eight Conditions for Lawful Processing

POPIA requires that all processing of personal information must comply with eight conditions set out in Chapter 3. The Company's approach to each condition is described below.

Condition 1 — Accountability

The Company takes full responsibility for ensuring that POPIA's conditions are met in all processing activities. Our Information Officer oversees compliance, and all staff with access to personal information are trained and accountable for adhering to this framework.

Condition 2 — Processing Limitation

Personal information is collected only for specific, explicitly defined, and lawful purposes. We do not process personal information in a manner that is incompatible with those purposes. Collection is limited to what is adequate, relevant, and not excessive for the purpose.

Condition 3 — Purpose Specification

The Company collects personal information for the following purposes:

- Providing, operating, and improving the Platform;
- Managing customer and user accounts and subscriptions;
- Processing payments and managing billing;
- Providing customer support and communicating service-related information;

- Complying with legal obligations;
- Conducting security monitoring and fraud prevention.

Personal information is retained only for as long as necessary to fulfil the purpose for which it was collected, or as required by law. Our retention schedule is set out in Section 7 below.

Condition 4 — Further Processing Limitation

Personal information will not be processed for a secondary purpose unless that purpose is compatible with the original purpose, the data subject has consented, or a legal ground exists. The Company does not sell personal information to third parties.

Condition 5 — Information Quality

The Company takes reasonable steps to ensure that personal information is complete, accurate, not misleading, and updated where necessary. Customers are encouraged to update their account information to maintain accuracy. Inaccurate data is corrected or deleted upon request.

Condition 6 — Openness

The Company is transparent about its processing activities. This is achieved through:

- This POPIA Compliance Framework (publicly available);
- Our Privacy Policy (available on the Platform and website);
- Just-in-time notices at the point of data collection;
- Our PAIA Manual, which describes how data subjects can access information held about them.

Condition 7 — Security Safeguards

The Company implements appropriate technical and organisational measures to secure personal information against loss, damage, unauthorised destruction, or unlawful access. These are described in detail in our Information Security Policy and include encryption, access controls, vulnerability management, and incident response procedures.

Condition 8 — Data Subject Participation

Data subjects have the right to know what personal information the Company holds about them, to request correction or deletion, and to object to certain processing. Our procedures for responding to data subject requests are set out in Section 5 below.

4. Lawful Grounds for Processing

Under POPIA, the Company relies on the following grounds (section 11) to lawfully process personal information:

Condition	Description / How We Rely On It
Consent	Where the data subject has given voluntary, specific, and informed consent (e.g., marketing communications, optional platform features).

Contractual necessity	Processing required to perform our contract with the Customer or to take pre-contractual steps at the data subject's request (e.g., account provisioning, billing).
Legal obligation	Where processing is required to comply with a legal obligation imposed on the Company (e.g., tax records, regulatory reporting).
Legitimate interest	Where the Company has a legitimate interest that is not overridden by the data subject's rights (e.g., platform security, fraud prevention, product improvement).
Vital interests	In rare cases where processing is necessary to protect the vital interests of the data subject or another person.

4.1 Special Personal Information

POPIA prohibits the processing of special personal information (section 26) unless specific conditions are met, including explicit consent or a statutory ground. The Platform is not designed to process special personal information by default. Customers who intend to process special personal information through the Platform must notify the Company in writing and obtain appropriate legal grounds before doing so.

Special personal information includes: religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric data, and criminal behaviour.

4.2 Children's Personal Information

The Platform is not directed at children (persons under 18). The Company does not knowingly collect personal information about children. Processing of children's personal information is prohibited without prior consent from a competent person (parent or guardian) as required by section 35 of POPIA.

5. Data Subject Rights

POPIA grants data subjects the following rights, which the Company is committed to upholding:

Data Subject Right	What It Means	How to Exercise
Right to access	Request a record of personal information held by the Company	Submit a PAIA request to privacy@[yourcompany].com
Right to correction	Request correction of inaccurate, incomplete, or outdated information	Email privacy@[yourcompany].com with details of the correction required

Right to deletion	Request deletion or destruction of personal information no longer needed or unlawfully processed	Email privacy@[yourcompany].com — subject to legal retention obligations
Right to object	Object to processing based on legitimate interests, or to direct marketing	Email privacy@[yourcompany].com or use in-platform opt-out settings
Right to complain	Lodge a complaint with the Information Regulator if you believe your rights have been violated	Contact the Information Regulator at inforeg@justice.gov.za

The Company will respond to all data subject requests within 30 days of receipt. Where the request is complex or the volume is high, the Company will notify the data subject of any extension within the initial 30-day period. Requests may be declined where a legal ground for refusal applies, in which case reasons will be provided.

6. Transfers of Personal Information

6.1 Transfers Within South Africa

Personal information shared with third-party operators within South Africa is subject to written agreements that impose POPIA-equivalent obligations on those operators.

6.2 Cross-Border Transfers

Section 72 of POPIA restricts the transfer of personal information outside South Africa unless the receiving country has adequate data protection laws, or appropriate safeguards are in place. Where the Company transfers personal information to third parties in other countries (e.g., cloud service providers), it ensures at least one of the following:

- The recipient country is on the Information Regulator's list of adequate jurisdictions;
- The data subject has consented to the transfer;
- The transfer is necessary for the performance of a contract;
- Binding contractual clauses or equivalent safeguards are in place.

A list of countries to which we may transfer personal information, and the safeguards applied, is available upon written request.

7. Retention and Destruction of Personal Information

Personal information is retained only for as long as necessary for the purpose for which it was collected or as required by applicable law. The Company's retention guidelines are as follows:

Category of Information	Retention Period	Basis

Customer account data	Duration of subscription + 3 years	Contractual obligation, legal compliance
Customer Data (uploaded content)	30 days post-termination (unless extended by agreement)	Contractual obligation
Financial & billing records	5 years from transaction date	Tax Administration Act, Companies Act
Security & access logs	Minimum 12 months	Security monitoring, legal compliance
Marketing consent records	Until consent is withdrawn + 3 years	POPIA section 11, evidence of consent
Employee personal information	Duration of employment + 5 years	Labour legislation, legal compliance

Upon expiry of the applicable retention period, personal information is securely destroyed or de-identified using methods appropriate to the medium (e.g., secure deletion for digital records, shredding for physical records).

8. Security Breach Notification

In the event of a security compromise that may result in the unlawful access to or acquisition of personal information (a 'security compromise'), the Company will comply with section 22 of POPIA as follows:

1. The Company will notify the Information Regulator as soon as reasonably possible after becoming aware of a security compromise.
2. The Company will notify affected data subjects unless the Information Regulator directs otherwise.
3. Notification will include: a description of the possible consequences of the compromise; the measures being taken to address the compromise; and recommendations for steps that data subjects can take to mitigate potential harm.
4. Where the Company acts as an operator, it will notify the responsible party (Customer) within 72 hours of becoming aware of the compromise, to enable the Customer to fulfil its own notification obligations.

Important
Security breach notification is a legal obligation under POPIA. Failure to notify may result in enforcement action by the Information Regulator.
To report a suspected breach to the Company: info@cmibridge.com

9. PAIA Manual

In accordance with the Promotion of Access to Information Act 2 of 2000 (PAIA), the Company has prepared a PAIA Manual that describes:

- The records held by the Company and how they may be accessed;
- The procedure for submitting access requests;
- The applicable fees;
- Grounds for refusal of access.

The PAIA Manual is available upon request from privacy@cmibridge.com. A copy will also be submitted to the South African Human Rights Commission as required.

10. Privacy by Design and Default

The Company embeds privacy into its processes, systems, and products from the outset. This means:

- Privacy Impact Assessments (PIAs) are conducted for new products, features, or processing activities that may impact personal information;
- Data minimisation principles are applied — only personal information strictly necessary for the purpose is collected;
- Privacy-protective defaults are applied where possible (e.g., opt-in rather than opt-out for non-essential processing);
- Third-party integrations and vendors are assessed for privacy compliance before adoption.

11. Staff Training and Awareness

All Company personnel with access to personal information are required to:

- Complete POPIA awareness training upon onboarding;
- Complete refresher training annually or when significant regulatory changes occur;
- Acknowledge and adhere to this framework and related internal policies;
- Report any suspected breach or non-compliance to the Information Officer immediately.

12. Complaints and Escalation

If you believe the Company has processed your personal information in violation of POPIA, you may:

5. Contact our Information Officer directly at privacy@cmibridge.com. We aim to resolve all complaints within 30 days.
6. If unsatisfied with our response, escalate your complaint to the Information Regulator of South Africa:

Information Regulator (South Africa)

Email: inforeg@justice.gov.za

Website: www.justice.gov.za/inforeg

Address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001

13. Review and Updates

This POPIA Compliance Framework is reviewed at least annually by the Information Officer, or earlier following:

- Material changes to the Company's processing activities;
- Amendments to POPIA or related regulations;
- Guidance issued by the Information Regulator;
- A significant security incident or compliance finding.

All updates to this framework are documented with version history and communicated to relevant stakeholders.

Document Owner: Information Officer | Review Cycle: Annual | Next Review: May 2027

This document does not constitute legal advice. [Creative Media Innovation (PTY) LTD] recommends engaging a qualified South African attorney to review your POPIA compliance programme.