Data Processing Agreement

[Creative Media Innovation (PTY) LTD] | CMI Bridge SaaS Platform
Effective Date: 7 May 2026

This Data Processing Agreement ('DPA') is entered into between [Creative Media Innovation (PTY) LTD] ('Processor') and the Customer identified in the applicable Order Form or Terms of Service ('Controller'). This DPA forms part of and is incorporated into the Terms of Service between the parties.

1. Definitions

- "Applicable Data Protection Law" means POPIA, GDPR (where applicable), and any other data protection law applicable to the processing of Personal Data under this DPA.
- "Personal Data" means any information relating to an identified or identifiable natural person processed by the Processor on behalf of the Controller.
- "Processing" has the meaning given to it under Applicable Data Protection Law and includes any operation performed on Personal Data.
- "Data Subject" means the individual to whom Personal Data relates.
- "Subprocessor" means any third party engaged by the Processor to process Personal Data on behalf of the Controller.
- "Security Incident" means any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

2. Scope and Role of the Parties

The Controller is the responsible party/controller of Personal Data submitted to the Platform. The Processor processes such Personal Data solely on behalf of the Controller, in accordance with the Controller's instructions and the terms of this DPA. The subject-matter, duration, nature, and purpose of the processing are set out in Schedule 1 to this DPA.

3. Controller's Obligations

The Controller warrants and represents that:

- It has a valid lawful basis for the collection and processing of Personal Data, including obtaining necessary consents from Data Subjects;
- It will provide Data Subjects with appropriate privacy notices as required by Applicable Data Protection Law;
- Its instructions to the Processor are and will remain compliant with Applicable Data Protection Law;
- It will promptly inform the Processor of any changes to the Personal Data it submits that may affect the Processor's compliance obligations.

4. Processor's Obligations

4.1 Instructions

The Processor shall process Personal Data only on documented instructions from the Controller. The Processor shall inform the Controller if any instruction infringes Applicable Data Protection Law.

4.2 Confidentiality

The Processor shall ensure that all personnel authorised to process Personal Data are subject to appropriate confidentiality obligations.

4.3 Security

The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including:

- Encryption of Personal Data in transit and at rest;
- Measures to ensure ongoing confidentiality, integrity, and availability of processing systems;
- A process for regularly testing and evaluating the effectiveness of security measures;
- Role-based access controls and multi-factor authentication.

4.4 Subprocessors

The Controller grants the Processor general authorisation to engage Subprocessors, provided that:

- The Processor imposes data protection obligations on Subprocessors equivalent to those set out in this DPA;
- The Processor remains liable for the acts or omissions of its Subprocessors;
- The Processor notifies the Controller of any intended changes to Subprocessors with at least 14 days' prior written notice, providing the Controller with the opportunity to object.

A list of current Subprocessors is available at [yourcompany.com/subprocessors] or upon written request.

4.5 Data Subject Rights

The Processor shall, to the extent technically feasible, assist the Controller in responding to Data Subject requests to exercise rights under Applicable Data Protection Law (such as access, rectification, deletion, and portability). The Processor shall promptly notify the Controller of any Data Subject request received directly.

4.6 Assistance with Compliance

The Processor shall provide reasonable assistance to the Controller with data protection impact assessments, prior consultation with supervisory authorities, and other compliance obligations, taking into account the nature of the processing.

5. Security Incidents

In the event of a Security Incident, the Processor shall:

- Notify the Controller without undue delay, and in any event within 72 hours of becoming aware of the incident;
- Provide sufficient information to allow the Controller to meet its own notification obligations;
- Take reasonable steps to mitigate and remediate the Security Incident.

The notification shall include (to the extent available): the nature of the incident, categories and approximate number of Data Subjects affected, likely consequences, and measures taken or proposed to address the incident.

6. International Data Transfers

Where the Processor transfers Personal Data to a country outside South Africa or the EEA that does not offer an equivalent level of data protection, such transfer shall be made subject to appropriate safeguards, including Standard Contractual Clauses (SCCs), binding corporate rules, or other mechanisms approved under Applicable Data Protection Law.

7. Audit Rights

The Processor shall make available to the Controller all information necessary to demonstrate compliance with this DPA and shall allow for and contribute to audits and inspections conducted by the Controller or a mandated auditor, subject to reasonable notice (not less than 30 days) and appropriate confidentiality obligations. Audit costs shall be borne by the Controller unless the audit reveals material non-compliance.

8. Deletion and Return of Data

Upon termination of the underlying Terms of Service, the Processor shall, at the Controller's option, delete or return all Personal Data and delete existing copies unless required by applicable law to retain such data. The Processor shall confirm deletion in writing within 30 days of receiving the instruction.

9. Liability

Each party's liability under this DPA is subject to and governed by the limitations of liability set out in the Terms of Service, except to the extent that any liability results from a party's breach of its obligations under Applicable Data Protection Law, in which case mandatory legal requirements shall apply.

10. Governing Law

This DPA shall be governed by the laws of the Republic of South Africa. Where the Controller is established in the EU and GDPR applies, the parties acknowledge that additional GDPR-specific requirements may apply, and agree to comply with such requirements.

Schedule 1: Details of Processing

Subject Matter:

Processing of Personal Data in connection with the provision of the Platform.

Duration:

For the duration of the Terms of Service and for any retention periods required under applicable law thereafter.

Nature and Purpose of Processing:

Processing of Personal Data to provide, maintain, and support the Platform, including user authentication, workflow management, reporting, and related operational functions.

Categories of Personal Data:

May include: names, email addresses, job titles, and any other personal information submitted by the Controller through the Platform in connection with process management activities.

Categories of Data Subjects:

The Controller's employees, contractors, clients, and other individuals whose data is submitted to the Platform by the Controller.

Special Categories of Data:

Not applicable by default. The Controller must notify the Processor before submitting any special category data (as defined under Applicable Data Protection Law) to the Platform.

This DPA is incorporated into and governed by the Terms of Service between the parties. In the event of any conflict, this DPA shall prevail in relation to the processing of Personal Data.