Data Processing Agreement

Fakade Innovations (Pty) Ltd, trading as M-Works™

Version 2.1 | Approved | Effective date 25/11/2026

1. Parties, purpose and application

This Data Processing Agreement (DPA) is between Fakade Innovations (Pty) Ltd (registration number 2024/044399/07), referred to as Fakade or M-Works, and the customer identified in the accepted service agreement (Client). It governs processing on the Client's behalf under the Protection of Personal Information Act 4 of 2013 (POPIA).

The parties accept this DPA and the completed processing schedule in writing or by valid electronic acceptance through their authorised representatives, together with the applicable service agreement. Mandatory law prevails. This DPA governs operator obligations if general or commercial terms conflict with it. A public copy or an enquiry alone does not constitute acceptance.

2. Definitions and roles

Personal information, processing, responsible party, operator and data subject have the meanings assigned in POPIA. A sub-operator is a third party engaged by Fakade to process personal information on the Client's behalf. Client Information means personal information processed by Fakade as operator under this DPA.

The Client determines the purposes and means of processing Client Information and is ordinarily the responsible party; Fakade acts as operator within documented instructions. Where a Client is itself an operator, the parties must confirm authority and applicable upstream instructions before processing.

Fakade acts separately as responsible party for its own enquiries, account administration, billing, legal obligations and independently determined security or business purposes, as applicable. Such processing is governed by law and the Corporate Privacy Notice, not by a blanket operator mandate.

3. Scope and documented instructions

Processing is limited to the accepted service, its agreed schedule and lawful documented instructions, including authorised support requests. The schedule specifies subject matter, duration, purposes, operations, information categories, data subjects, recipients, transfers and exit arrangements. Changes must be documented and agreed before expanded processing.

Fakade will not sell Client Information, use it for unrelated marketing, or use it to train general-purpose AI models. If an instruction appears unlawful or exceeds the agreed scope, Fakade will inform the Client and may pause the affected processing pending clarification. Where law requires processing beyond instructions, Fakade will notify the Client where permitted.

4. Client responsibilities

The Client warrants that it has a lawful ground for processing Client Information, the rights and authorisations needed to supply it and instruct Fakade, and any consent required by law. The Client must give required collection notices, respect data subject rights, ensure accuracy and necessity, and issue lawful documented instructions. It must authorise access, protect credentials, promptly report suspected compromises and identify special personal information, children's information or other high-risk processing before introducing it.

The Client must identify any legally required authorisations or restrictions. The parties will cooperate to assess additional safeguards and, where applicable, prior authorisation under POPIA before the relevant processing begins.

To the extent permitted by law, the Client indemnifies Fakade for amounts lawfully payable on a third-party claim and reasonable, necessary defence costs only to the extent directly caused by a breach of this warranty or the Client's unlawful instructions. Fakade must promptly notify the Client, allow reasonable participation in the defence and take reasonable steps to mitigate loss. The indemnity does not cover a regulatory fine or penalty imposed on Fakade or loss to the extent caused by Fakade's unlawful conduct, negligence or contractual breach. It does not limit any statutory right, duty or remedy that cannot lawfully be limited.

5. Confidentiality and security

Fakade will establish and maintain appropriate, reasonable technical and organisational safeguards in accordance with sections 19–21 of POPIA. It will identify reasonably foreseeable internal and external risks, maintain safeguards against them, regularly verify their effectiveness and update safeguards as risks change. It will have due regard to generally accepted security practices and applicable industry requirements.

Access to Client Information will be restricted to authorised persons with a legitimate service need, bound by confidentiality. Disclosure is limited to authorised processing or legal requirements. Confidentiality continues after the end of access or the agreement.

Controls will be proportionate to the service and risk, including encrypted transmission, access management and authentication, appropriate separation of customer data, secure configuration, vulnerability management, logging, incident response and backup or recovery arrangements where applicable. The applicable schedule and agreed security records specify the controls used; this clause is not a certification or absolute guarantee of security.

6. Sub-operators and international transfers

The Client authorises only the categories of sub-operators identified in the accepted schedule or agreed provider register. Fakade will identify the actual providers, processing locations and functions, give reasonable advance notice of material changes, and allow the Client to raise reasonable data protection objections before the change. The parties will seek a suitable alternative or agree a lawful resolution under the service agreement.

Fakade will impose appropriate written confidentiality, security, incident notification, instruction and return or deletion obligations on sub-operators, and remains responsible to the Client for fulfilling its own obligations under this DPA. Providers acting as independent responsible parties must be distinguished from sub-operators.

Processing outside South Africa requires documented authorisation and a lawful transfer condition under section 72 of POPIA where applicable. Fakade will cooperate in assessing protections, onward transfers and any necessary prior authorisation, and will not initiate an unapproved transfer. A provider's global availability is not evidence of a lawful transfer arrangement.

7. Security compromises

Fakade will notify the Client immediately if it has reasonable grounds to believe that an unauthorised person accessed or acquired Client Information, as required by section 21(2) of POPIA. Fakade will give the initial notice using the information then available and will take reasonable steps to contain, investigate and mitigate the compromise and preserve relevant evidence.

Fakade will supply further information as it becomes available and aims to provide a supplementary report within 24 hours of the initial notification where reasonably practicable. Updates will cover, where known, the nature and timing of the compromise, affected information and data subjects, likely consequences, response actions and a follow-up contact. The Client is responsible for its notifications under section 22, with prompt assistance from Fakade. Where Fakade is the responsible party, it fulfils its own statutory notification duties.

8. Rights requests, assistance and assurance

Fakade will promptly refer requests concerning Client Information to the Client, unless legally required or expressly authorised to respond, and reasonably assist with access, correction, deletion, objections, complaints, security assessments, investigations and regulatory enquiries. It will make relevant records and information available to demonstrate compliance with this DPA.

On reasonable written request, Fakade will provide proportionate assurance evidence and cooperate with justified audits, subject to confidentiality, security and protection of other customers. The parties will agree scope and timing; urgent incidents and lawful regulatory powers are not restricted by these arrangements.

9. Retention, return and deletion

Fakade will retain Client Information only as necessary for authorised processing or another lawful retention ground. On expiry or termination, Fakade will follow documented Client instructions to return or securely delete it within the agreed schedule, subject to applicable law. If the Client has not issued instructions, Fakade will seek them and restrict further processing to necessary protection, return, deletion or legally required retention.

Where retention is required by law, access and use will be restricted to that purpose. Residual backup copies will be protected, excluded from ordinary use and removed through the agreed backup expiry cycle; if restored, applicable deletion instructions must be reapplied. Fakade will confirm completion of return or deletion on reasonable request. Product schedules govern formats and timelines; the Pages website archive is not automatic authority to retain visitor records.

10. Liability, duration and communications

This DPA applies while Fakade processes Client Information, including authorised exit processing. Confidentiality, security, incident cooperation and return or deletion duties survive as needed. Liability is governed by the applicable accepted service agreement, subject to expressly agreed data-protection provisions and mandatory law. Nothing excludes liability for fraud, wilful misconduct, gross negligence or any statutory right, duty, liability or remedy that cannot lawfully be excluded.

Information Officer: Ulwazi Mapukata | privacy@m-works.co.za. The Client will designate a privacy and incident contact in its order or schedule. Formal contractual notices and service of legal proceedings are subject to the applicable service agreement and law. The General Terms of Service set out the common notice mechanics. South African law governs this DPA.

The parties will record the identities and authority of their accepting representatives, the acceptance method and date and time, and the exact service agreement, DPA and completed schedule versions. They may rely on electronic acceptance where permitted by law and will comply with any legally prescribed form or signature requirements.

Schedule A — PAM

Payroll Aggregation by M-Works™ | Processing schedule

Applicability: activate only for the agreed PAM deployment and supported functionality. Complete the deployment-specific details before acceptance.

A1. Subject matter, purpose and duration

Processing of employee and payroll information to provide payroll calculations, payroll run management, payslip generation, reporting, statutory compliance support, authorised integrations and customer support. Processing lasts for the agreed service term and authorised exit or retention period.

A2. Data subjects and information

- Employees and other payees where applicable: names, identifiers, contact and employment details, remuneration, allowances, deductions, statutory contributions, tax and payroll records, and bank details where required for authorised functionality.
- Client administrators and authorised users: account identifiers, contact and role information, access and audit records. Special personal information or children's information, if needed, requires a separate documented assessment and instructions.

A3. Processing and recipients

Agreed operations may include import, validation, calculation, storage, retrieval, reporting, authorised export, transmission and deletion. Recipients may include authorised Client personnel, approved hosting and technical providers, and authorised banks, payment providers or statutory authorities where the relevant integration is enabled. Payment execution remains with the appointed bank or provider under the Client's authority; this DPA does not authorise Fakade to hold or transfer Client funds.

A4. Security and transfer arrangements

Record actual hosting region, database and backup locations, privileged access, role controls, audit logging, encryption, tenant or environment separation, and approved integration providers in the deployment register. Restrict access to payroll and bank information; avoid including unnecessary identifiers or payroll content in general logs or notifications. Verify all external transfers and contract safeguards before activation.

A5. Exit and retention

Agree the export formats, delivery method, active-data deletion deadline and backup expiry before processing. The Client remains responsible for retaining required payroll and statutory records. Fakade will retain data only on lawful documented instructions or where required by law. The Pages 90-day archive rule does not apply to PAM.

Activation details to complete

Client/contact; deployment and enabled modules; information categories; provider and location register; approved security controls; export, deletion and backup timelines; authorised payment/statutory integrations, if applicable.

Schedule B — M-Works Pages

Managed website design and hosting | Processing schedule

Applicability: activate for the agreed customer website and functionality. A simple static site and a site receiving visitor records may require different instructions.

B1. Subject matter, purpose and duration

Design, publication, hosting, maintenance, agreed content changes and technical support. Where instructed, Fakade may process information for enquiry or booking features. Processing lasts for the service term and authorised exit period. Fakade's own Pages sales enquiries, subscriptions and billing are separate responsible-party activities.

B2. Data subjects and information

- Client representatives, staff or other persons identified in supplied website content: business contact details, names, biographies, photographs and other authorised content.
- Website visitors and prospective customers: network and security metadata and, only where agreed features collect it, contact details, enquiry messages, order or booking request details. The Client must identify any sensitive or children's information before enabling such collection.

B3. Operations and recipients

Authorised operations may include receiving and editing content, hosting and public display as instructed, maintenance, security monitoring and delivering visitor enquiries where enabled. Direct WhatsApp links may route a visitor to the Client or messaging provider without Fakade storing the message; verify per site. Identify approved hosting, form, notification and domain providers and any analytics configuration. Planned payment collection for Pages subscriptions is not an active operator feature.

B4. Security and exit

Record actual hosting and backup locations, access restrictions, form routing, provider agreements and transfer safeguards. Public content must be separated from private visitor information. Following cancellation or termination, the website implementation may be retained securely for 90 calendar days under the subscription agreement for restoration, buyout or free retrieval of supplied content.

The archive must exclude visitor enquiries, booking records, exports and logs unless a separate lawful retention ground and documented instructions permit retention. Personal information embedded in site content must also be assessed. Limit archive access; remove or return information on the agreed timeline, subject to law. A buyout includes only authorised transferable files and assets, not secrets, unrelated customer data or private provider credentials.

Activation details to complete

Client/contact; site address; enabled forms and analytics; provider/location register; public and private data categories; visitor-data return/deletion and backup deadlines; archive access and deletion owner.

Schedule C — Tshapisa

White-label storefront | Prospective processing schedule

Status: planning draft only. This schedule does not establish that Tshapisa or any listed capability is live. Approve and complete it against the actual deployment before processing customer information.

C1. Intended subject matter and purposes

Potential provision of branded storefronts, merchant administration, product and service listings, and authorised customer interactions. Additional order, booking, payment and courier integrations are subject to separate design, assessment and agreement. Duration will be defined in the accepted product agreement and exit schedule.

C2. Potential data subjects and categories

- Merchant representatives and authorised staff: contact, account and role information, business details and access records.
- Merchant customers and visitors: contact and delivery details, enquiry, order or booking information, preferences, and technical or security metadata, only where required by enabled functionality.
- Payment references, transaction status and delivery records may be processed if the relevant integrations are implemented and approved. No authority is granted here to collect or retain full payment-card credentials or unrelated sensitive information.

C3. Roles, operations and recipients

The merchant will ordinarily determine the purposes of its customer-facing processing; Fakade may act as operator for hosting and agreed storefront functions. Roles must be mapped separately for merchant account administration, payments, couriers, fraud checks and analytics. Potential operations include authorised collection, storage, display, order or booking management, transmission, export and deletion. Providers must be identified and classified before activation.

C4. Security and transfer safeguards

Define and validate tenant isolation, access controls, authentication, secure integration credentials, event and audit logging, storage locations, backups and incident procedures. Assess payment and courier data minimisation, provider contracts, cross-border transfers and any required authorisation. No proposed provider is approved by this draft.

C5. Return, deletion and activation

Specify merchant exports, delivery method, retention and deletion deadlines, backup expiry and treatment of customer records on exit. Do not apply the Pages archive rule automatically. Complete the Client/contact, enabled functionality, information categories, roles, approved providers and regions, security measures, processing duration and exit arrangements before written acceptance.