Data Processing Agreement

Controller processor terms for Stocklane customer data

Provider: [Stocklane Legal Entity Name]

Prepared: 30 September 2026

Effective date: [Effective Date]

Document status: Pre publication legal template

Complete every bracketed field and obtain legal advice from counsel qualified in each market before publishing or signing this document.

This Data Processing Agreement forms part of the agreement between [Stocklane Legal Entity Name] (Stocklane or Processor) and the customer accepting it or signing an Order Form (Customer or Controller). It governs Stocklane's processing of Personal Data on the Customer's documented instructions while providing the Stocklane retail operations service.

1 Purpose and roles

For Customer Data that the Customer, its authorised users, staff, customers, suppliers or loyalty members enter into the Service, the Customer is the Controller and Stocklane is the Processor. The Customer determines the purposes and means of that processing.

Stocklane acts as an independent Controller for account administration, security, service usage, legal compliance, billing and its direct relationship with the Customer. This Agreement does not govern that independent processing; the Stocklane Privacy Policy does.

The parties will comply with applicable data protection law, including the Nigeria Data Protection Act 2023 where applicable, and any mandatory data protection law applicable to the processing.

2 Documented instructions

Stocklane will process Customer Data only to provide, secure, maintain and support the Service, to comply with this Agreement and the Customer's documented lawful instructions, or where required by applicable law. Stocklane will notify the Customer before following a legal requirement unless law prevents that notice.

The Customer warrants that it has a lawful basis for its instructions and for all Customer Data it places in the Service, including staff data, customer loyalty data, purchase history, contact details and uploaded product images.

3 Confidentiality and access

Stocklane will restrict access to Customer Data to personnel and authorised sub-processors who need it to provide the Service, are bound by confidentiality obligations, and are subject to appropriate access controls. Stocklane will not sell Customer Data or use it for unrelated advertising.

4 Security

Stocklane will maintain appropriate technical and organisational measures that are proportionate to the risks of the processing. The current baseline is described in Schedule 2. The Customer remains responsible for its authorised-user permissions, endpoint security, password practices, branch operations and the accuracy of data entered into the Service.

5 Sub processors and international transfers

The Customer gives Stocklane general written authorisation to appoint sub-processors necessary to provide the Service, provided Stocklane imposes materially equivalent data protection obligations and remains responsible for their performance to the extent required by law or the Principal Agreement.

Stocklane will make its current sub-processor categories available on request and will provide reasonable advance notice of a material new sub-processor where applicable law requires it. The Customer may object on reasonable data-protection grounds; the parties will work in good faith on a solution, failing which the Customer may terminate the affected Service without penalty.

Where Customer Data is transferred across borders, the parties will use an applicable lawful transfer mechanism and supplementary safeguards where required.

6 Assistance and data subject requests

Taking account of the nature of processing, Stocklane will provide reasonable assistance to help the Customer respond to a valid request from a data subject, supervisory authority, or regulator. If Stocklane receives a request relating to Customer Data, it will direct the requester to the Customer where appropriate and will not respond except as required by law or authorised by the Customer.

Stocklane will provide reasonable information available to it to assist with data protection impact assessments, prior consultations, compliance enquiries and audits, subject to confidentiality, security, and reasonable cost controls.

7 Personal data incident

Stocklane will notify the Customer without undue delay after becoming aware of a confirmed Personal Data Incident affecting Customer Data. The notice will contain available information reasonably needed for the Customer to assess notification duties, and Stocklane will provide reasonable cooperation as the investigation develops.

The Customer is responsible for deciding whether to notify individuals, regulators, staff, customers, or business partners unless Stocklane is legally required to do so itself.

8 Audits and evidence

No more than once each twelve months, or following a substantiated incident or regulator request, the Customer may request reasonable information demonstrating Stocklane's compliance with this Agreement. Any audit must be on reasonable notice, during normal business hours, protect other customers and Stocklane confidential information, and avoid disruption. The Customer bears its audit costs unless the audit identifies material non-compliance by Stocklane.

9 Return deletion and retention

On termination, the Customer may export Customer Data using available Service functionality during the applicable access period. Stocklane will then delete or return Customer Data in accordance with its retention schedule, except where law requires retention or data remains in protected backups until the next scheduled overwrite cycle. Retained data will remain protected and will not be used for a new purpose.

10 Liability and precedence

The liability, indemnity, governing law, dispute resolution and limitation provisions of the Master Services Agreement apply to this Agreement. If this Agreement conflicts with the Principal Agreement on processing of Customer Data, this Agreement controls to the extent of that conflict.

Schedule 1 Details of processing

Topic	Details
Subject matter	Provision of multi-tenant retail operations, including inventory, branches, point of sale, staff access, reporting, customer loyalty and support.
Duration	For the term of the applicable Service and the retention period described in this Agreement.
Nature and purpose	Hosting, storing, displaying, securing, supporting, exporting and processing Customer Data solely to operate the Service.
Data subjects	Customer administrators, authorised users, employees, contractors, customers, loyalty members, suppliers and other persons whose data the Customer enters.
Personal data	Names, business contact details, usernames, roles, branch access, loyalty contacts and consent records, sales and purchase references, inventory records, audit logs, support communications and uploaded images.
Special categories	Not intended. The Customer must not place special-category data, government identifiers, full payment-card details or other highly sensitive data in the Service unless expressly agreed in writing.

Schedule 2 Baseline security measures

• Tenant and business separation, role-based permissions and branch or warehouse access controls.

• Authentication controls, password protection, secure account recovery and audit logging for privileged operational actions.

• Encryption in transit where supported, controlled infrastructure access and secure configuration management.

• Input validation, file-type and file-size controls for supported product and branding uploads, and security testing proportionate to the service risk.

• Operational resilience measures, incident handling, backup and restoration procedures appropriate to the deployed environment.

• Security review whenever a material new processor, tracking technology, payment feature or personal-data use is introduced.