

KLARI TECHNOLOGIES LIMITED

Data processing addendum

This is the binding version of this document as published in the Klari Trust Centre. The same text is rendered at klari.ng/trust.

VERSION	Version 1
EFFECTIVE	18 Sept 2026
DOCUMENT HASH	038eb259 ede4bc01 f1fb77b7 32d97a5e 5cc4cf9b 56084e48 51cc06ea 05435218

Data Processing Agreement

KLARI TECHNOLOGIES LIMITED

Effective date: 18 September 2026

Important notice

This Data Processing Agreement (the "**DPA**") forms part of, and is incorporated into, the Klari Terms of Service, any Master Services Agreement, any Order Form or any other agreement governing the supply of the Service by Klari Technologies Limited (the "**Principal Agreement**").

It governs the Processing of Personal Data by Klari Technologies Limited on behalf of its Customers and is intended to record the obligations of a Data Processor under the Nigeria Data Protection Act 2023, the General Application and Implementation Directive 2025 and the regulations, directives and guidance issued by the Nigeria Data Protection Commission.

This DPA requires a completed Annex A before it is executed. The parties' legal names, the processing details, the supplier list and the cross-border transfer schedule must be completed and agreed for the particular Customer before Customer Personal Data is Processed. This document without a completed Annex A is a template, not an executed agreement.

Customers requiring a separately executed copy may contact Klari at **hello@klari.ng**.

1. Parties and principal agreement

This DPA is entered into between:

KLARI TECHNOLOGIES LIMITED, a private company limited by shares incorporated under the laws of the Federal Republic of Nigeria with registration number RC 9542173, whose registered office is in Lagos, Nigeria ("**Klari**" or the "**Processor**");

AND

the organisation subscribing to or using the Klari platform, as identified in Annex A (the "**Customer**" or the "**Controller**").

Each a "**Party**" and together the "**Parties**".

The Parties' legal names, registered addresses, notice contacts, authorised signatories and effective date are completed in Annex A and in the Principal Agreement. Where this DPA and the Principal Agreement conflict, the signed Principal Agreement controls, except where applicable data protection law requires a different result, in which case this DPA controls to the extent of that requirement.

2. Definitions

In this DPA:

"Applicable Data Protection Law" means the NDPA, GAID, and any regulation, directive, code, guidance note or decision issued under them, together with any other data protection law applicable to a Party's Processing under this DPA.

"**Controller**" means the entity that determines the purposes and means of Processing Personal Data.

"**Customer Personal Data**" means Personal Data contained within Tenant Data that Klari Processes on the Customer's behalf under this DPA.

"**Data Subject**" means the natural person to whom Personal Data relates.

"**GAID**" means the General Application and Implementation Directive 2025.

"**NDPA**" means the Nigeria Data Protection Act 2023.

"**NDPC**" or the "**Commission**" means the Nigeria Data Protection Commission.

"**Personal Data**" means any information relating to an identified or identifiable natural person.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of or access to Personal Data.

"**Processing**" means any operation performed on Personal Data, including collection, recording, storage, organisation, retrieval, consultation, use, disclosure, transmission, restriction, erasure or destruction.

"**Processor**" means the entity that Processes Personal Data on behalf of a Controller.

"**Sensitive Personal Data**" means any category of Personal Data designated as sensitive under the NDPA, including data revealing health, biometric or genetic data, race or ethnic origin, religious or political beliefs, trade union membership, sexual orientation, or criminal records.

"**Service**" means the Klari software platform and the related services supplied under the Principal Agreement.

"**Sub-processor**" means a third party engaged by Klari to Process Customer Personal Data.

"**Tenant Data**" means data the Customer or its authorised users upload to or generate within the Service.

3. Subject matter, purpose and duration

Klari Processes Customer Personal Data solely to supply the Service to the Customer as described in the Principal Agreement, and on the Customer's documented instructions.

Nature of the Processing. Hosting, storage, structured retrieval, organisation, transformation, transmission, presentation, backup and secure deletion of compliance records maintained by the

Customer through the Service, including Records of Processing Activities, Data Protection Impact Assessments, evidence files, the audit log and generated dossiers.

Purpose of the Processing. To enable the Customer to maintain its own compliance records, document its own assessments, preserve its own audit trail and generate exportable materials for its own review, approval and regulatory processes.

Duration. This DPA remains in force for as long as Klari Processes Customer Personal Data on the Customer's behalf. Processing ceases on termination of the subscription, subject to the export window and the return and deletion provisions in clause 15.

4. Details of the Processing

Categories of Data Subject — Klari's own Processing to run the account. The Customer's authorised users, administrators and billing contacts.

Categories of Data Subject — within the Customer's compliance records. Any category of individual the Customer chooses to describe or record in its Records of Processing Activities, Data Protection Impact Assessments or evidence, which may include the Customer's employees, directors, contractors, consultants, vendors, customers, applicants, shareholders, beneficial owners, website visitors and business partners.

Categories of Personal Data — Klari's own Processing to run the account. Name, work email address, organisation membership and role, authentication records, and audit log entries recording the actor, action, resource, timestamp, IP address, user agent and request identifier of each state-changing action.

Categories of Personal Data — within the Customer's compliance records. Any Personal Data the Customer chooses to record, which may include names, contact details, employment information, regulatory and compliance records, technical identifiers, correspondence, and supporting evidence and attachments.

Sensitive Personal Data. Klari does not seek Sensitive Personal Data for its own purposes. Where the Customer records Sensitive Personal Data in its compliance documents, Klari Processes it solely on the Customer's documented instructions and applies the same isolation and storage controls described in clause 9 and Annex B.

The Customer determines the content. Klari does not determine what Personal Data the Customer uploads to the Service. Responsibility for establishing and recording a lawful basis for the Processing of that Personal Data rests solely with the Customer as Controller.

5. Controller obligations

The Customer shall:

1. ensure that every instruction it gives Klari is lawful and consistent with Applicable Data Protection Law;
1. establish and maintain a valid lawful basis for its Processing under NDPA s.25, and record it;
1. provide all notices and obtain all consents that Applicable Data Protection Law requires of it;
1. ensure that Personal Data it submits to the Service is accurate, relevant and limited to what is necessary for the compliance record being created;
1. respond to Data Subject requests addressed to it, except where it expressly requests assistance from Klari under clause 12;
1. comply with clause 7 (data the Customer must not submit); and
1. remain solely responsible for determining the purposes and means of its Processing.

The Customer warrants that it has all rights, permissions, authorisations and lawful bases necessary to instruct Klari to Process Customer Personal Data.

Before Processing begins, the Customer shall give Klari the information reasonably needed to understand its documented instructions, data categories, Data Subjects, processing locations and material risks. Where relevant to Klari's Processing, the Customer shall share the outcome of its Data Protection Impact Assessment and any risk controls it requires Klari to apply.

6. Processor obligations

Klari shall:

1. Process Customer Personal Data only on the Customer's documented instructions, including as to transfers, unless required to do otherwise by law, in which case Klari shall inform the Customer of that requirement before Processing, unless the law prohibits it;
- 1.

ensure that persons authorised to Process Customer Personal Data are bound by enforceable confidentiality obligations;

1. implement and maintain the technical and organisational measures described in clause 9 and Annex B;
1. engage Sub-processors only in accordance with clause 11;
1. assist the Customer as set out in clause 12;
1. notify the Customer of a Personal Data Breach in accordance with clause 13;
1. make available the information reasonably necessary to demonstrate compliance with this DPA, as set out in clause 14;
1. return or delete Customer Personal Data in accordance with clause 15; and
1. cooperate with the Commission and any other competent supervisory authority where legally required to do so.

Use of the Service is an instruction from the Customer only to the extent that it is consistent with this DPA, the Principal Agreement and Applicable Data Protection Law.

Klari shall inform the Customer if, in its opinion, an instruction infringes Applicable Data Protection Law. Klari is not obliged to provide legal advice, and informing the Customer under this clause is not a legal opinion.

7. Data the Customer must not submit

The Service holds records **about** Processing activities, not the operational data those activities concern.

The Customer shall not submit to the Service, whether in a free-text field or an uploaded evidence file, payment transaction records, payment references, settlement or routing data, payment card numbers, CVV/CVC values, PINs, one-time passcodes, authentication credentials or secrets for any system, full bank account details beyond what is strictly necessary to describe a Processing activity, or Sensitive Personal Data that is not necessary for the compliance record being created.

Klari cannot rely on this restriction alone: data the Customer uploads is data Klari Processes, and the restriction does not undo that. The restriction exists so that neither Party inadvertently engages the Customer's sector-specific localisation, security or retention obligations by placing operational payment data into the Service.

Where Klari becomes aware that prohibited data has been submitted, Klari may, where technically practicable and proportionate, quarantine it, restrict access to it, redact it or delete it, and shall notify the Customer where reasonably practicable. Klari does not systematically monitor Customer content and gives no undertaking to detect every instance.

8. Confidentiality

Klari shall ensure that every employee, contractor, consultant and other person authorised to access Customer Personal Data is bound by enforceable confidentiality obligations, whether contractual or statutory.

Those obligations survive the termination of the individual's employment or engagement, and survive the termination of this DPA.

Klari shall ensure that access to Customer Personal Data is limited to personnel who require it to perform their duties.

9. Security measures

Klari shall implement and maintain technical and organisational measures appropriate to the risks presented by the Processing, taking account of the state of the art, the cost of implementation and the nature, scope, context and purposes of the Processing.

The baseline measures for the engagement are set out in **Annex B**. Klari shall provide the current version to the Customer on request and shall add technical detail where the Customer's Processing, its Data Protection Impact Assessment or an applicable sector rule requires it.

Klari shall review those measures periodically and update them where necessary to maintain a level of security appropriate to the risk.

Klari's public security description at <https://klari.ng/security> is explanatory. It does not replace the measures agreed in this DPA, and where they differ the measures agreed in Annex A or Annex B govern.

10. International transfers

Annex A must be completed on this clause before execution.

Tenant Data is intended to be hosted in **Frankfurt, Germany (eu-central-1)**. Application compute is configured for the same region. Limited service metadata may be Processed by suppliers in other locations, as disclosed in Annex A.

Klari is a Nigerian company whose infrastructure is in Germany. Accordingly, use of the Service can involve a transfer of Personal Data out of Nigeria, and that transfer is the one governed by Part VIII of the NDPA.

The applicable transfer mechanism is under review with Nigerian privacy counsel and is not settled. Klari will not describe a transfer mechanism as approved, adequate or settled until that review is complete. In particular, Klari does not rely on, and does not assert, any adequacy decision of the Commission in respect of the European Economic Area or Germany.

Cross-border Processing must not be treated as covered by a settled mechanism in this template. The applicable NDPA and GAID safeguard, any approval required from the Commission, the transfer assessment, and the recipient and onward-transfer restrictions must be completed in the transfer schedule in Annex A and agreed by the Parties before Customer Personal Data is Processed.

Klari shall provide the Customer with the supplier, location, transfer and security information reasonably needed for the Customer's own transfer assessment. The Customer remains responsible for its controller-side lawful basis and instructions. Klari remains responsible for the processor obligations it accepts in the executed DPA.

Klari shall not transfer Customer Personal Data to a location not disclosed in Annex A without the Customer's prior written authorisation, except where required to do so by law.

11. Sub-processors

The Customer authorises Klari to engage the Sub-processors identified in the executed Annex A for hosting, infrastructure, storage, communications, authentication, error monitoring, abuse prevention and support.

Before execution, Klari shall give the Customer the current named list, together with each Sub-processor's role, location, the categories of Personal Data it can access and the security

terms that apply to it. Klari maintains that list and makes it available through its Trust Centre and on request at privacy@klari.ng.

Klari shall carry out appropriate due diligence on each Sub-processor and shall impose written data protection terms on it that are no less protective than those in this DPA, including onward-transfer restrictions.

Notice and objection. Klari shall notify the Customer before appointing a new Sub-processor where Applicable Data Protection Law or the Principal Agreement requires it. Where an addition or replacement materially changes the location of the data or the category of access, Klari shall give at least **fourteen (14) days'** notice, and the Customer may object in writing within that window, stating its reasons. The Parties shall work in good faith towards a reasonable resolution; if none is available, the Customer may exercise any termination right in the Principal Agreement.

Klari remains responsible for the acts and omissions of its Sub-processors in relation to the Processing of Customer Personal Data as if they were its own.

12. Assistance to the Controller

Taking account of the nature of the Processing and the information available to it, Klari shall provide reasonable assistance to the Customer in:

1. responding to a request from a Data Subject exercising a right under the NDPA;
1. carrying out a Data Protection Impact Assessment, a prior consultation or a risk assessment;
1. notifying a Personal Data Breach to the Commission or to affected Data Subjects; and
1. engaging with the Commission or another competent supervisory authority.

Where the Service provides an export, report or log that satisfies a request, supplying it is sufficient assistance for these purposes. Klari may charge for assistance that is substantial and outside the ordinary operation of the Service, at rates agreed in advance in writing.

13. Personal Data Breach notification

Klari shall notify the Customer without undue delay, and in any event **within twenty-four (24) hours**, after becoming aware of a Personal Data Breach affecting Customer Personal Data, so that the Customer can meet its own **72-hour** notification obligation to the Commission under NDPA s.40.

The twenty-four hour period runs from the moment Klari becomes aware of a Personal Data Breach, not from the moment one occurs. Nothing in this clause is a commitment to detect an incident within a given time. Klari's breach-response governance, including its stated current constraints, is published at <https://klari.ng/trust/breach-response>.

A notification shall describe, so far as it is then known, the nature of the breach, the categories and approximate volume of Personal Data and Data Subjects concerned, the likely consequences, the measures taken or proposed, and a contact point. Where the full picture is not available at once, Klari shall provide information in phases without further undue delay.

Klari shall cooperate with the Customer and take the reasonable steps the Customer requires to assist its investigation, mitigation and remediation.

14. Audit rights

The Customer may, on reasonable written notice and no more than once per calendar year, request a written audit response covering Klari's security measures, its Sub-processors, its relevant policies, and the information reasonably needed to demonstrate compliance with this DPA. Klari shall respond within thirty (30) days.

Klari shall provide its current compliance or registration information where that is applicable to its role.

The Customer may audit more frequently where Applicable Data Protection Law requires it, or following a Personal Data Breach affecting the Customer's Personal Data.

Any on-site audit, independent assessor or expanded assurance work must be agreed by the Parties in writing in advance, including its scope, confidentiality terms, timing and cost. Each Party bears its own costs unless otherwise agreed.

15. Return and deletion

On termination of the subscription, Klari shall make the Customer's Tenant Data available for export for **thirty (30) days** through the export functions the Service provides. On written request within that window, Klari shall supply a complete copy of the Tenant Data as a machine-readable archive at no charge.

After the export window closes, Klari shall delete the Tenant Data in accordance with the agreed retention schedule, except to the extent that:

- 1.

retention is required by applicable law, in which case Klari shall retain only what the law requires, for only as long as it requires it, and shall continue to protect it under this DPA; or

- 1. the data remains in a secure backup until the next scheduled overwrite, in which case it is isolated from active Processing and deleted on that overwrite.

The Customer may request earlier deletion in writing. Klari shall comply unless it has a lawful basis for retaining the data, and shall in that case explain what it cannot delete and why.

The retention periods that apply to Klari’s own Controller records — account records and the audit log — are those disclosed in the Privacy Notice and are not overridden by this clause.

16. General

Liability. The Principal Agreement governs liability, indemnity, insurance, force majeure, notices, amendment and dispute resolution, except where this DPA expressly provides otherwise or Applicable Data Protection Law requires a different result.

Governing law. This DPA is governed by the laws of the Federal Republic of Nigeria, and the dispute resolution provisions of the Principal Agreement apply to it.

Order of precedence. Annex A, once completed and agreed, prevails over the body of this DPA on the matters it addresses.

No incompatible use. Neither Party shall use Personal Data in a way that is incompatible with this DPA, the documented instructions or Applicable Data Protection Law.

Severability. If a provision of this DPA is held unenforceable, the remainder continues in force and that provision is to be read down to the minimum extent necessary to make it enforceable.

Annex A — Processing, supplier and transfer schedule

This annex must be completed and agreed for the particular Customer before this DPA is executed and before Customer Personal Data is Processed.

ITEM	REQUIRED COMPLETED INFORMATION
Controller	Customer legal name, registered address, privacy/DPO contact and authorised signatory

Processor	Klari Technologies Limited, registered address, privacy contact and authorised signatory
Principal Agreement	Order Form / Terms / MSA title, date and version
Processing purpose and scope	The specific features, data categories, Data Subjects and documented instructions agreed with the Customer
Processing duration	Subscription term plus the agreed export, deletion and legally required retention periods
Processing locations	Each country or region where the Processor or a Sub-processor will Process Customer Personal Data, including any edge or support metadata processing
Sub-processors	Name, role, location, data categories, security terms and onward-transfer restrictions for every authorised Sub-processor
Transfer mechanism	The counsel-approved NDPA/GAID mechanism, any required Commission approval, the transfer assessment date and the supporting documents
Material risks and DPIA outcome	The Customer's relevant risk assessment, DPIA outcome and any additional controls or restrictions Klari must follow
Customer instructions	Any sector-specific restriction, retention limit, data minimisation rule or security control that supplements this DPA

The Parties shall update this annex before a material change to a processing location, supplier, transfer mechanism, data category or material risk takes effect.

Annex B — Baseline technical and organisational measures

The Parties shall confirm the following measures for the engagement and record any Customer-specific additions in Annex A:

- access controls, authentication and role-based authorisation;
- separation between customer tenancies, with access controls enforced in the database so that a user reaches only their own organisation's data;

- encryption in transit, and encryption at rest for stored data and files;
- private file storage reachable only through short-lived signed links;
- an append-only activity history preserving a record of material changes;
- exported PDFs stamped with a SHA-256 of the data they were rendered from, so that alteration is detectable — this is tamper-evidence, not a digital signature, and does not prove who produced a document;
- incident detection, response, escalation and processor-to-customer notification procedures;
- backup, restoration, retention and secure-deletion procedures;
- confidentiality commitments and staff and contractor access controls;
- logging, change management and periodic review proportionate to the Processing risk; and
- supplier due diligence, written processor terms and onward-transfer controls.

Klari shall provide the current supporting information reasonably necessary for the Customer's review. The Parties shall add technical detail where the Customer's Processing, its Data Protection Impact Assessment or an applicable sector rule requires it.

No security measure can guarantee absolute security. Klari's current security description, including its stated limitations, is available at <https://klari.ng/security>.