KLARI TECHNOLOGIES LIMITED

Privacy notice

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 8
EFFECTIVE	6 Oct 2026
DOCUMENT HASH	83bca5a3 1ec1572e 109787c8 6c0eb1ed 40aa4760 391d7429 6475da0f 07f2b957

Privacy Notice

KLARI TECHNOLOGIES LIMITED

Effective date: 6 October 2026

Issued under the Nigeria Data Protection Act 2023 ("**NDPA**") and the General Application and Implementation Directive 2025 ("**GAID**").

1. Who we are

Klari Technologies Limited ("**Klari**", "we", "us", "our") is 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.

Depending on the processing activity, Klari acts in one of two capacities.

1.1 As Data Controller. Klari determines the purposes and means of processing, and is the Data Controller, for personal data collected through the Klari marketing website (https://klari.ng), and for account administration, customer support, contracts, billing, service security and business communications.

1.2 As Data Processor. Klari acts as Data Processor for Tenant Data — the compliance records a customer puts into the product and directs us to process on its behalf. In that case the customer remains the Data Controller, Klari processes the data only on the customer's documented instructions, and Klari does not determine the purposes of that processing. The terms are set out in our Data Processing Agreement.

This notice describes what we do in both capacities and says which is which.

For privacy enquiries write to **privacy@klari.ng**.

2. Definitions

- **Personal data** — any information relating to an identified or identifiable natural person.
- **Sensitive personal data** — data revealing health, biometric or genetic data, race or ethnic origin, religious or political beliefs, trade union membership, sexual orientation, or criminal records, or any other category designated as sensitive under the NDPA.
- **Processing** — any operation performed on personal data, from collection and storage through to disclosure, erasure and destruction.
- **Data subject** — the individual to whom the personal data relates.
- **Data Controller** — the person who determines the purposes and means of processing.
- **Data Processor** — the person who processes personal data on a Controller's behalf.
- **Tenant Data** — the data a customer or its authorised users upload to or generate within the Klari product.

3. What we collect and why

Lawful bases below are cited to the NDPA. The Act sets them out at section 25(1): paragraph (a) is consent, and paragraph (b) sub-paragraphs (i) to (v) are contract, legal obligation, vital interest, public interest and legitimate interest respectively.

3.1 Marketing site visitors

- **"Request access" form:** name, work email, organisation, role, free-text message, submission IP address. We use this to evaluate prospective design partners and to reply to enquiries. Lawful basis: _legitimate interest in business development_ (NDPA s.25(1)(b)(v)).
- **Operational logs:** request paths, response codes, IP address, user agent. Used for security and abuse prevention only. These logs are held by our hosting and error-monitoring providers and are retained for those providers' standard periods, which we do not currently override; we can confirm the current windows on request. Our error monitoring is configured not to attach IP addresses or request headers. Lawful basis: _legitimate interest in service security_ (NDPA s.25(1)(b)(v)).

3.2 Authenticated users

- **Account data:** email address (for sign-in), display name, organisation membership and role. We use this to provide the account, administer the customer relationship and protect access to the Service. Lawful basis: _performance of a contract_ and, where appropriate, _legitimate interest in service security_.
- **Audit log:** every state-changing action in your tenant produces an append-only event recording the actor's email, the action, the resource, the timestamp, the IP address, the user agent and the request identifier. This is part of the product, not analytics. Lawful basis: _performance of the Service_ and _legitimate interest in security, integrity and accountability_. We may also retain a record where a specific legal obligation applies.
- **Department reminders:** if your organisation makes you the owner of a department, Klari emails you when a colleague asks you to complete that department's records and, if your organisation switches it on, once a week while they remain incomplete. Each reminder is recorded with who it went to and when, and appears in your organisation's audit log. Klari only sends reminders to people who have a Klari account and have consented to their data being stored in Germany. Lawful basis: _performance of a contract_ (NDPA s.25(1)(b)(i)).
- **Support requests:** when you raise a request under Help & support, we keep your email address, your organisation, the subject and message you write, the area and priority you choose, and when the request was raised, acknowledged and resolved. Everyone in your organisation with a Klari account can see the requests raised for it, including the message. We send two emails: a notification to our business mailbox, whose reply-to is your address, and a confirmation to you. Our reply and anything after it is ordinary email. The audit log records that a request was raised, acknowledged or resolved, with its reference, priority and area —

not its subject or message. We use this to answer you and to keep a record of when each request was answered. Please describe the problem rather than copying personal data from your compliance records into a request, unless we ask for it. Lawful basis: _performance of a contract_ (NDPA s.25(1)(b)(i)) and _legitimate interest in keeping a record of the service we provide_ (NDPA s.25(1)(b)(v)).

3.3 Tenant Data

Where a customer uses the product, the platform processes whatever personal data that customer records in its compliance documents — for example the categories of data subject described in a Record of Processing Activities, or personal data contained in an uploaded evidence file.

We process that data solely as Data Processor, on the customer's documented instructions. We do not determine what a customer uploads, and we do not use Tenant Data for our own purposes.

3.4 Sensitive personal data

We do not seek sensitive personal data for our own purposes. Where a customer, acting as Data Controller, records sensitive personal data in its compliance documents (for example in a Record of Processing Activities or a Data Protection Impact Assessment), Klari processes it solely on that customer's documented instructions and applies the same tenant isolation and storage controls described in section 8.

3.5 What we do not collect

We do not run third-party analytics, advertising trackers or session-replay tools on klari.ng. **We do not sell personal data.** We do not profile users for marketing. We make no decision about anyone based solely on automated processing.

4. Who we share it with

We do not sell personal data, and we do not disclose it for any other party's independent purposes. We disclose personal data only:

- to the sub-processors described in section 9, under the applicable data processing terms and only for operating the Service;
- to professional advisers such as lawyers or auditors, under confidentiality, where reasonably necessary;
- to regulators, courts or law-enforcement agencies where we are legally required to do so.

Where we receive a legally binding demand for personal data, we disclose only what the demand requires, and we notify the affected customer where we are lawfully able to do so.

5. Where the data lives, and international transfers

Core Tenant Data — organisation records, evidence and the activity history — is intended to be stored in **Frankfurt, Germany (eu-central-1)** with our hosting and storage sub-processors. Application compute is configured for the same region. Network routing can read limited session information at the edge in order to direct a request, but is not intended to read, write or retain a compliance record.

Klari is a Nigerian company whose infrastructure is in Germany, so use of the Service can involve a transfer of personal data out of Nigeria. The relevant provider categories, locations and data access are disclosed in section 9.

The lawful transfer mechanism is under review with Nigerian privacy counsel and is not settled. That review covers whether an NDPC-approved Cross-Border Data Transfer Instrument or another documented mechanism is required. **Klari will not describe a transfer mechanism as approved, adequate or settled until that review is complete, and does not rely on any adequacy decision of the Commission.** Before a customer signs or begins processing Tenant Data, Klari provides the then-current transfer terms, recipient information and documented assessment relevant to that customer.

Your own account data. Before you use the Service, we ask for your consent to your own personal data — your name, email address, any contact details you enter about yourself (such as a Data Protection Officer's phone number and qualifications) and the record of your activity — being transferred to and stored in Germany, and we explain the risks when we ask (NDPA s.43(1)(a)). You can withdraw that consent at any time from your profile settings, after which you can no longer use the Service. Withdrawing does not affect processing that has already happened.

6. How long we keep it

- **"Request access" submissions:** the content you type is not stored in Klari — the form sends two emails and writes no row to our database. One notifies us; one confirms back to the address you entered, so you have a record of what you sent. Your submission therefore persists in our business mailbox and in our email provider's sending logs, under their retention periods, and we delete enquiries from the mailbox once they are closed. **Your IP address is included only in the notification to us, never in the confirmation to you.** It is otherwise held for about

an hour as an abuse-prevention counter (see section 9), which is what stops the form being flooded.

- **Account data:** for the life of the contract, and then for the period required to meet applicable business, accounting, tax or legal obligations.
- **Audit log:** retained for the life of the tenant plus seven years. An audit trail is only worth anything if it outlives the dispute it might be needed for, and a Compliance Audit Return can be examined well after the period it covers. Customers may export their log at any time.
- **Support requests:** for the life of the contract, then deleted with your organisation's data on the timetable below. The audit events that record them follow the audit-log period above. Copies of the emails sit in our business mailbox and in our email provider's sending logs; we delete them from the mailbox when the contract ends, and the provider's logs expire under its own retention period.
- **Operational logs:** as set out in section 3.1.

How this fits with deletion on termination. Our contract terms say that when a subscription ends we make your tenant data available for export for 30 days and then delete it. That means the working product data — your organisation record, Records of Processing Activities, Data Protection Impact Assessments, evidence files, dossiers and support requests. It does not override the two retention periods above, which continue to apply to account records and to the audit log. If you need those destroyed earlier, write to privacy@klari.ng and we will tell you what we can delete, what we must keep, and why.

7. Your rights

The NDPA gives you the following rights. We do not charge for exercising them.

- **Confirmation and information** — to know whether we process personal data about you and, if we do, the purposes, the categories of data, who receives it (including recipients in other countries), how long we keep it, where we got it, and whether any automated decision-making is involved (s.34(1)(a)).
- **A copy of your data** in a commonly used electronic format (s.34(1)(b)).
- **Correction** of personal data that is inaccurate, out of date, incomplete or misleading — or its deletion where correction is not feasible or suitable (s.34(1)(c)).
- **Erasure** without undue delay (s.34(1)(d)). We must also erase on our own initiative where the data is no longer necessary for the purpose it was collected for, or where we have no other lawful basis to keep it (s.34(2)).
- **Restriction of processing** while a request is being resolved, while an objection is outstanding, or where the data is needed for legal claims (s.34(1)(e)).

- **Withdrawal of consent** at any time, where consent is the lawful basis. Withdrawing is as easy as giving it, and does not affect processing that has already happened (s.35).
- **Objection** to processing (s.36). Where we rely on legitimate interest we will stop unless we can demonstrate overriding grounds. For direct marketing you may object at any time and we must stop (s.36(3)–(4)).
- **Not to be subject to a decision based solely on automated processing** that produces legal effects concerning you or similarly significantly affects you (s.37). We make no such decisions.
- **Data portability** — where the right applies to the processing at issue, you may ask for your data in a structured, commonly used electronic format. We will assess and respond to the request in line with the Act and GAID, including the rights of other people.
- **Complaint to the regulator** — you may complain to the Nigeria Data Protection Commission (s.46) at https://ndpc.gov.ng. You do not have to come to us first.

The Act requires us to act "without constraint or unreasonable delay". We commit to responding to a verified request **within 30 days**, and to telling you inside that period if a request is genuinely complex and will take longer. Send requests to privacy@klari.ng.

Where Klari is the Processor. If your personal data is in a customer's compliance records, that customer is the Controller and is responsible for answering your request. Tell us and we will direct you to them and assist them as our Data Processing Agreement requires.

8. Security

Klari applies technical and organisational measures designed to protect personal data, including:

- **Separation between customers**, with access controls enforced in the database so that users reach only their own organisation's data.
- **An activity history** designed to preserve records of material changes.
- **Private file storage**, reachable only through short-lived signed links.
- **Encryption in transit**, and encryption at rest for stored data and files.
- **Exported PDFs stamped with a SHA-256** of the data they were rendered from, so alteration is detectable. This is tamper-evidence, **not** a digital signature: it shows a document has changed, it does not prove who produced it.
- **Authentication and authorisation checks** for changes to customer data.

No security measure can guarantee absolute security. The current security description, **including its material limitations**, is available at https://klari.ng/security. We publish that page because an

honest account of what is not yet in place is more useful to a Data Protection Officer than a list of controls.

9. Sub-processors

We use a small set of sub-processors. The current named list, their service categories, locations and data access is available at https://klari.ng/security and is versioned in the Trust Centre. We provide the current list to prospective and existing customers on request at privacy@klari.ng or security@klari.ng.

We notify customers of a new sub-processor before it is engaged where applicable law or our contract requires, and give at least **14 days' notice** where an addition materially changes the data location or the category of access.

10. If something goes wrong

If we detect a personal data breach affecting your data, we contain it, assess the risk, and investigate the cause.

- **Where Klari acts as Processor**, we notify the affected customer without undue delay and within **24 hours** of becoming aware, so that the customer can meet its own **NDPA s.40 72-hour** notification obligation.
- **Where Klari is the Controller** and the breach is likely to result in a risk to data subjects, we notify the Commission within the applicable **72-hour** period.
- **Where a breach is likely to result in a high risk** to data subjects, we communicate with the affected people without undue delay, in clear language, and provide practical protective information.

Our full breach-response policy, including an honest statement of our current detection constraints, is published at https://klari.ng/trust/breach-response.

11. Children

Klari is a workplace compliance tool and is not intended for anyone under 18. We do not knowingly collect personal data from minors; if we learn that we have, we delete it promptly.

12. Changes to this notice

We post a revised effective date when this notice changes. Every previous version stays available in the Trust Centre at https://klari.ng/trust/privacy, each pinned to the SHA-256 of the text that was in force, so you can check what applied on any given date.

Where a change materially affects how we process your personal data, we will take reasonable steps to bring it to your attention rather than relying on publication alone.

13. Contact

Klari Technologies Limited (RC 9542173) Lagos, Nigeria

Privacy enquiries and data subject requests: **privacy@klari.ng** Security and breach reports: **security@klari.ng** General enquiries: **hello@klari.ng**

Klari is assessing its Data Protection Officer obligations with Nigerian counsel. If a Data Protection Officer is appointed or required, the contact details will be published here and communicated as applicable law requires.

If you are dissatisfied with our response, you may lodge a complaint with the:

Nigeria Data Protection Commission (NDPC) https://ndpc.gov.ng