

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 1
EFFECTIVE	11 May 2026
DOCUMENT HASH	5e3b7bcd 926718d5 d9255e7c d8e28a09 f3397fee d0bf21fc 5fd53255 77260ee8

Privacy notice

Issued under the Nigeria Data Protection Act 2023 and the General Application and Implementation Directive 2025.

1. Who we are

Klari Technologies Limited (“**Klari**”, “we”, “us”) is a private company incorporated in Nigeria. We are the Data Controller for personal data we collect via the Klari marketing website (<https://klari.ng>) and the Data Processor for personal data our customers (Nigerian organisations classified under the NDPC Major Importance regime) entrust to Klari when using our product.

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, deletion, 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.

3. What we collect and why

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 reply to enquiries. Lawful basis: *_legitimate interest in business development_* (NDPA s.25(c)).
- **Operational logs:** request paths, response codes, IP address, user-agent. Used for security and abuse prevention only; retained 90 days. Lawful basis: *_legitimate interest in service security_*.

3.2 Authenticated users

- **Account data:** email address (for sign-in), display name, organisation membership, role. Lawful basis: *_performance of a contract_* (NDPA s.25(b)).
- **Audit log:** every state-changing action in your tenant produces an append-only event: actor email, action, resource, timestamp, IP, user-agent, request ID. This is part of the product, not analytics. Lawful basis: *_compliance with a legal obligation_* (NDPA s.25(d)) — audit trails are required for NDPA s.34 audits.

3.3 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 RoPA or DPIA), Klari processes it solely on that customer's documented instructions and applies the same tenant isolation and storage controls described in section 8.

3.4 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.

4. Who we share it with

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

- to the sub-processors listed at <https://klari.ng/trust/sub-processors>, under data-processing terms (see section 9 — all are EU-resident);
- 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.

5. Where the data lives

All tenant data — your organisation, records, evidence, audit log — is stored exclusively in **Frankfurt, Germany (eu-central-1)** on Supabase Postgres + Storage. Application compute runs on Vercel functions pinned to the same region. No tenant data is held by a US- or non-EU CDN.

Cross-border data flows to a non-Nigerian jurisdiction (Germany) are conducted under standard data protection clauses with our infrastructure providers, as contemplated by NDPA s.43, and rely on the recognition under NDPA s.41 that the European Economic Area provides an adequate level of protection. We can produce the current clause sets on request for NDPC submission.

6. How long we keep it

- **“Request access” submissions:** 12 months from submission, then destroyed unless converted to a customer relationship.
-

Account data: for the life of the contract plus the retention window required by Nigerian financial-services law for related business records (currently six years; superseded by sector-specific requirements where stricter).

- **Audit log:** retained for the life of the tenant plus seven years, as standard for NDPA s.34 audit defensibility. Customers may export their log at any time.
- **Operational logs:** 90 days.

7. Your rights

Under the NDPA you may:

- request a copy of personal data we hold about you (s.36);
- request correction of inaccurate or incomplete data (s.36);
- request deletion where retention is no longer lawful (s.37);
- object to processing based on legitimate interest (s.36);
- withdraw consent at any time, where consent is the lawful basis (s.26);
- lodge a complaint with the Nigeria Data Protection Commission at <https://ndpc.gov.ng>.

We respond to verified rights requests within 30 days. Send them to privacy@klari.ng.

8. Security

Klari is built around five hardening rules documented in our architecture: tenant-scoped row-level security on every table; an append-only audit log enforced at the database layer; private storage with signed URLs and short download TTLs; signed PDF exports; and a single mutation chokepoint that re-checks authentication on every state-changing call. Secret keys are server-only and never shipped to the browser.

9. Sub-processors

We use a small, EU-resident set of sub-processors. The current list is available on request to privacy@klari.ng and is also published at <https://klari.ng/trust/sub-processors>. We will notify customers of any addition that materially changes data location or category of access at least 14 days in advance.

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 your Processor we notify you without undue delay — within 24 hours of becoming aware — so you can meet your own NDPA s.40 72-hour notification clock. Where the law requires it, we notify the NDPC and affected individuals. Our full procedure is set out in our Data Breach Response Policy.

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 will post a revised effective date when this notice changes. The previous version remains available on request for audit purposes (and on the Trust Centre at <https://klari.ng/trust/privacy/v/N>).

13. Contact

Klari Technologies Limited Privacy enquiries: privacy@klari.ng General: hello@klari.ng