

KLARI TECHNOLOGIES LIMITED

Data breach response policy

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	0fa3f61e 34f8b64d 07fc9824 017cfdc8 89e2da7e 43e413dd e5ae5e59 a93f612a

Data Breach Response Policy

KLARI TECHNOLOGIES LIMITED

Effective date: 18 September 2026

1. Introduction

Klari Technologies Limited ("Klari", "the Company", "we", "us", "our") treats the confidentiality, integrity and availability of personal data as fundamental to the product we sell. We build compliance software for organisations that are themselves accountable under the Nigeria Data Protection Act 2023 ("NDPA"), and we hold ourselves to the standard we help them meet.

Despite technical and organisational safeguards, information security incidents and personal data breaches can occur through cyber threats, system vulnerabilities, human error, malicious activity, operational failure or events outside our control. This policy establishes how we identify, contain, investigate, report and remediate an actual or suspected personal data breach.

2. Purpose

The purpose of this policy is to provide a consistent and coordinated approach to the management of personal data breaches and information security incidents across Klari's operations, so that:

1. incidents are detected and reported promptly;
1. they are assessed and investigated properly;
1. harm to affected individuals and organisations is minimised;
1. Klari meets its obligations under the NDPA, the General Application and Implementation Directive 2025 ("GAID") and its contractual commitments to customers; and
1. what we learn from an incident changes what we do next.

3. Scope

This policy applies to all personal data, confidential information and information assets that Klari processes, manages, stores or transmits.

It applies where Klari acts as **Data Processor** on behalf of a customer, and where Klari acts as **Data Controller** for its own business operations.

It applies to everyone who works on Klari's behalf — employees, directors, contractors, consultants, advisers and sub-processors — and to information held in any environment, including production databases, object storage, backups, cloud infrastructure, business email, endpoint devices and third-party services.

4. Policy statement

Klari does not conceal, suppress or delay the reporting of an incident.

Every suspected or actual breach is reported, assessed and investigated without undue delay, and is managed with accountability, proportionality and confidentiality.

Failure by a member of staff or a contractor to report a known incident is a disciplinary matter.

5. What counts as a breach

A personal data breach is any event leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data. Examples include:

- unauthorised access to customer or account data;
- disclosure of personal data to an unintended recipient;
- loss or theft of a device or credential giving access to personal data;
- a cyberattack such as ransomware, malware or account takeover;
- a misconfigured store or access rule exposing data;
- unauthorised modification or deletion of records;
- loss of availability of personal data caused by a system failure.

Whether a given event is a reportable breach is decided after assessment under section 7, not assumed.

6. Detection and reporting

Anyone who becomes aware of a suspected or actual incident must report it immediately to **privacy@klari.ng**. Security-specific reports may go to **security@klari.ng**. Both addresses are monitored, and both accept reports from outside Klari — including from customers, researchers and members of the public.

Reports may also originate from monitoring and alerting, a customer report, an audit finding or a third party.

A report should include whatever is known: the nature of the incident, the systems involved, when it was discovered, the data potentially affected, and any action already taken. An incomplete report made promptly is better than a complete one made late.

The current privacy contact position is set out in our Privacy Notice. Any appointed or legally required Data Protection Officer contact will be published there and in this policy.

7. Assessment and investigation

On receipt of a report, Klari promptly assesses the incident to establish:

- whether a personal data breach has in fact occurred;
- the categories and volume of data involved;
- the number of data subjects potentially affected;
- the systems and assets impacted, and the duration of exposure;
- the root cause;
- the likelihood and severity of harm to data subjects; and
- any legal, contractual or regulatory implications.

Where useful, forensic steps are taken to preserve evidence. Investigations are conducted confidentially and documented.

8. Containment, mitigation and recovery

Where a breach is confirmed or reasonably suspected, Klari acts immediately to contain it — for example by revoking credentials, disabling compromised accounts, isolating affected systems, rotating secrets or applying temporary controls.

We then remediate the underlying cause, restore affected services, recover data where possible, and strengthen controls to reduce the chance of recurrence, while preserving evidence for the investigation.

9. Notification

A breach may trigger legal, contractual or regulatory notification duties.

9.1 To customers, where Klari is Processor. Where a breach affects a customer's data, Klari notifies that customer without undue delay and in any event **within 24 hours** of becoming aware, so that the customer, as Controller, can meet its own **NDPA s.40 72-hour** notification obligation to the Nigeria Data Protection Commission ("**NDPC**"). This matches the commitment in our Data Processing Agreement.

9.2 To the NDPC, where Klari is Controller. Where a breach of Klari's own data is likely to result in a risk to data subjects, Klari notifies the NDPC within the applicable **72-hour** period.

9.3 To affected individuals. Where a breach is likely to result in a high risk to affected people, Klari communicates with them without undue delay, in clear language, including practical steps they can take to protect themselves.

9.4 Content. A notification carries enough detail for the recipient to understand the incident, assess the risk and take protective steps: the nature of the breach, the categories and approximate volume of 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, we provide information in phases rather than delaying the first notification.

10. Record-keeping

Klari maintains a breach register recording every reported incident — whether or not it results in regulatory notification — including its nature, the dates of occurrence and discovery, the actions taken, the decisions made, the notifications issued, the remediation applied and the lessons learned.

Records are retained in line with our legal and regulatory obligations.

11. Post-incident review

After an incident is resolved, Klari reviews the root cause, the adequacy of existing controls, and the timeliness and effectiveness of the response, and implements corrective actions.

Findings feed back into our controls, testing and training.

12. Governance, and an honest statement of our current capacity

Ownership of this policy and of the breach-response process sits with Klari's founder today, and passes to the Data Protection Officer on designation. The response to any given incident is led

by that person and draws in engineering and, where relevant, legal counsel and the affected customer.

We state the current constraint rather than implying a team that does not exist:

Klari is a one-person engineering organisation with no on-call rota and no 24/7 security monitoring.

Two consequences follow, and we would rather a customer read them here than discover them during an incident:

1. The 24-hour customer notification commitment in section 9 runs from the moment we **become aware** of a breach, not from the moment one occurs. Nothing in this policy is a commitment to detect an incident within a given time.
1. We do not claim a standing incident-response team spanning security, legal, communications and customer success. As Klari grows, these roles will be formalised, and this section will be updated to describe what actually exists at that point. The process set out above applies regardless of headcount.

13. Training and awareness

Klari gives staff and contractors periodic training on their incident-reporting responsibilities, updated to reflect changes in law, regulatory guidance and our own systems.

14. Review of this policy

This policy is reviewed at least annually, and sooner where law, regulatory guidance, our systems or our organisational capacity change materially.

Every previous version stays available in the Trust Centre at <https://klari.ng/trust/breach-response>, each pinned to the SHA-256 of the text that was in force.

15. Contact

Klari Technologies Limited (RC 9542173) Lagos, Nigeria

Breach and privacy reports: **privacy@klari.ng** Security reports: **security@klari.ng** General enquiries: **hello@klari.ng**

Owner of this policy: Founder, Klari Technologies Limited **Approved by:** Management