Privora

PRIVACY OPERATIONS · PRIVORA PRO · RUNBOOK

Run a personal data breach response with accountable decisions

Run one time-aware response with clear authority, reviewed facts, recorded decisions, and traceable follow-up.

Primary action

Open the client breach register in Privora Pro.

Version
1.0.0

Reviewed
2026-08-12

Guide
Open the Privora guide

CONTROLLED OPERATIONAL RESOURCE

Important legal and use notice

Review these conditions before relying on or sharing this document.

GUIDE
Open the Privora guide

VERSION
1.0.0

REVIEWED
2026-08-12

Purpose

This document is a Privora operational resource designed to help teams organize privacy work, evidence, ownership, review, and reporting.

No guarantee

Use of this document or Privora does not guarantee compliance with any law, regulation, standard, or contractual obligation.

Generated and reviewed material

This document was generated by Privora from the canonical operating kit identified on this page. Human review remains required before the document is relied upon or shared.

Use and intellectual property

Not legal advice

This document provides general operational guidance. It is not legal advice and does not replace advice from qualified legal or regulatory professionals.

Current requirements

Laws, regulatory guidance, product workflows, and organizational obligations may change. Users are responsible for confirming the current requirements that apply to their circumstances before acting.

Data handling

Do not enter personal, sensitive, privileged, or confidential information into uncontrolled copies. Store approved operational records only in authorized systems and follow your organization's access, retention, and handling policies.

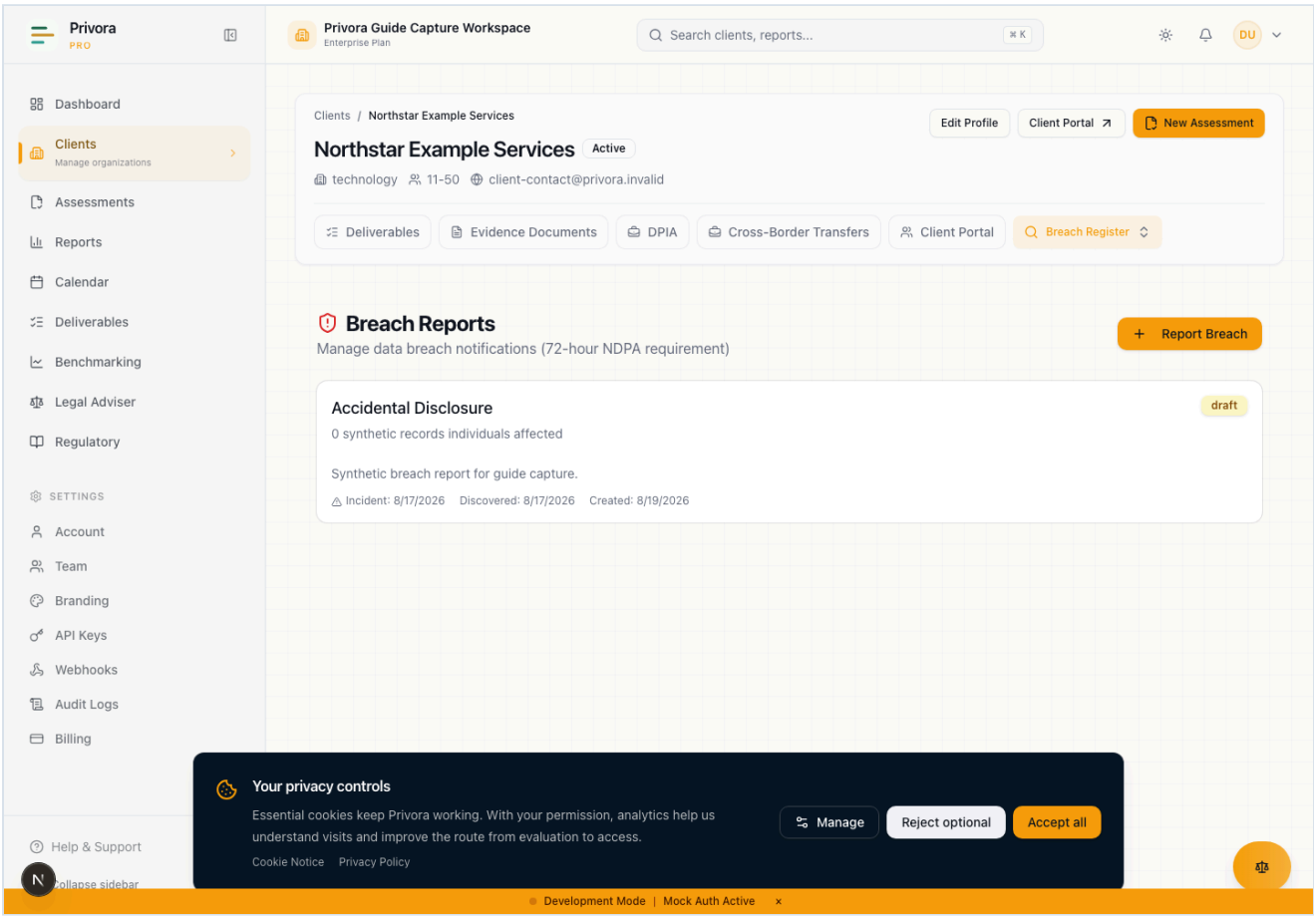
Change notice

This document reflects the version and reviewed sources identified on this page. Product workflows and authoritative guidance may change, and a later release may supersede this document.

Run a personal data breach response with accountable decisions

Product walkthrough

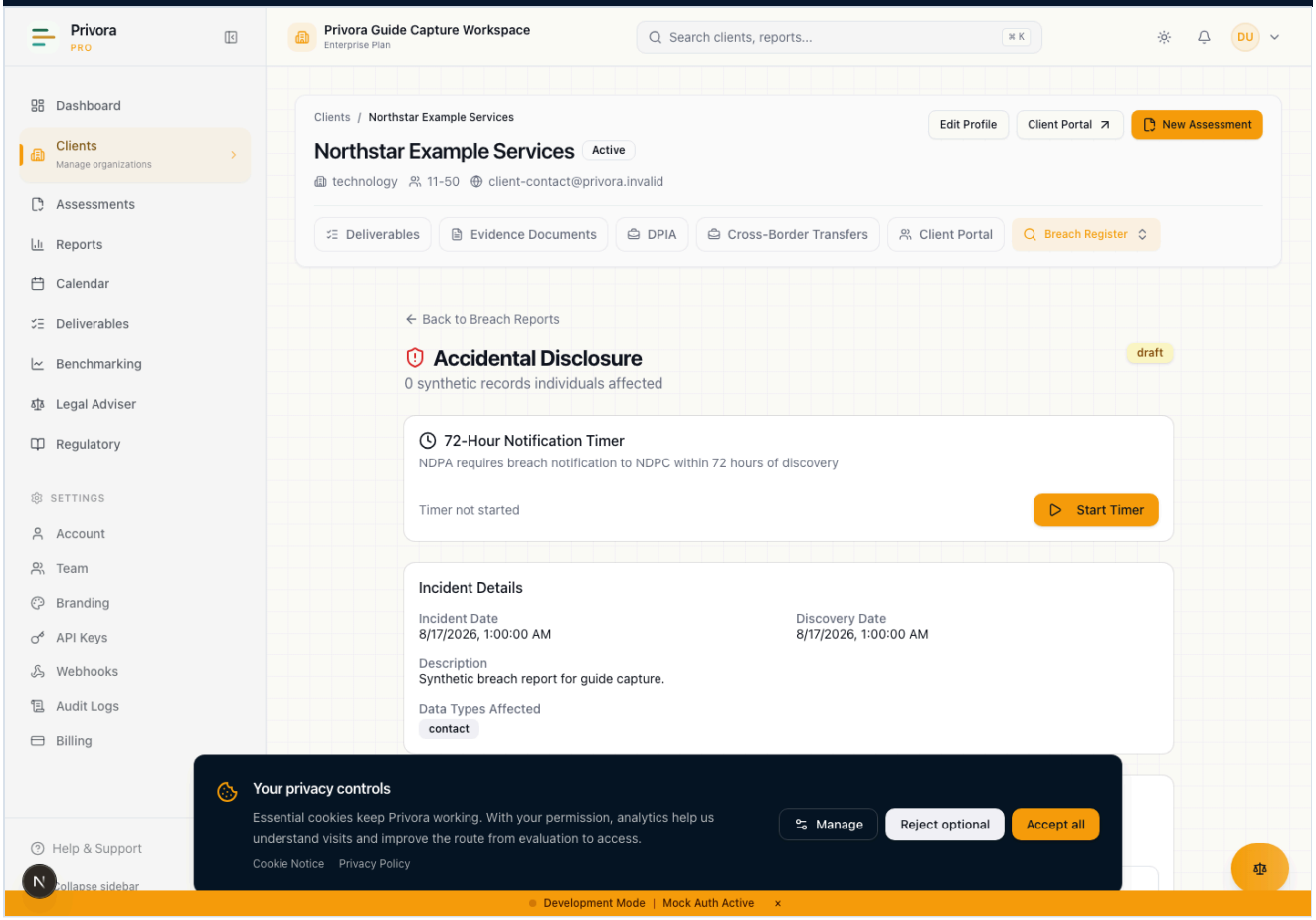
Open the client workspace, select Breach, and use the register and incident detail pages to keep facts, decisions, owners, and follow-up together. Use Calendar for review points and the portal task only for assigned client contributions. The product records the work; accountable people still make and approve the external decision.



Use the Console breach list view to continue the privacy operations workflow.
1. Breach heading

How to reach this page

1. Start on the Console dashboard
2. Open the breach list workflow



Use the Console breach detail view to continue the privacy operations workflow.
1. Breach report heading

> Operational guidance — not legal advice. This guide does not guarantee compliance. Privora Pro does not file, submit, send, or lodge regulatory notices automatically.

This runbook supports professional incident and Privacy Operations work. It does not replace qualified legal or regulatory review, determine risk automatically, or prove that a notice was filed. Apply the facts, the Nigeria Data Protection Act 2023, current Nigeria Data Protection Commission guidance, applicable contracts, and any separately verified sector obligations with accountable human judgment.

Treat the blank runbook and workbook as internal working material. Keep live incident records, personal data, forensic material, credentials, system images, and communications in approved systems with need-to-know access. Enter only the approved operational record in the correct Privora Pro client workspace.

The operating outcome

A breach response succeeds when the team can show a controlled path from awareness to containment, risk assessment, notification decision, communication, remediation, and review. The objective is not merely to complete a form. It is to protect people, reduce continuing harm, meet applicable duties, and preserve a review-ready record of facts and accountable decisions.

This workflow improves a high-pressure handoff for Nigerian DPCOs, DPOs, client incident leads, security teams, and management reviewers. It is better than coordinating through email and disconnected documents because each stage names an owner, input, output, decision gate, and operating record. It reduces complexity by keeping the response timeline, evidence references, decision rationale, communications, and follow-up connected to one client and one incident.

The required outputs are a verified awareness time, an incident record, containment status, an evidence index, an assessment of risk to rights and freedoms, a controller notification decision, a data-subject communication decision, approved communications where required, remediation ownership, and a post-

incident review. Uncertainty is expected. Record what is known, what is estimated, what is disputed, who is resolving the gap, and when the decision will be revisited.

Privora Pro is the operating record after approved information is entered. The system helps organize the work; it does not make the legal decision, send a notice to the Commission, or replace incident command. Human owners remain accountable for accuracy, authority, external delivery, and evidence of delivery.

Activate the workflow at awareness

Activate the workflow when a person with responsibility for the controller becomes aware of facts indicating that a security failure may have caused accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. Do not wait for a complete forensic conclusion before establishing the record and assigning response owners. Also do not label every security event a personal data breach without checking whether personal data and a breach of its security are involved.

Capture the awareness time separately from the suspected incident time and discovery time. Awareness is a fact to verify, not a date selected to make a deadline convenient. Record the source of the alert, the role that received it, the earliest confirmed escalation, and any disagreement about when controller awareness occurred. If a processor reported the event, retain the processor's notice and identify when the controller received enough information to begin its assessment.

Open the client breach register and create a draft record with the safest useful summary. Use a neutral incident reference rather than a person's name. Record categories and estimates instead of copying raw affected records. Set the immediate containment owner, privacy decision owner, evidence coordinator, communications owner, and management reviewer. Confirm how the team will communicate securely and who may see forensic or identity-bearing material.

> A controller notifies the Commission within 72 hours after becoming aware of a breach when the breach is likely to result in a risk to the rights and freedoms of individuals. Where feasible applies to the notice details, not to the notification window. Missing information may be provided in phases without undue delay. High-risk communication to affected data subjects is immediate.
>
> Reviewed 2026-08-12 against the linked source material.

> **Treat the statutory period as continuous**
>
> The product timer is an operational aid; pausing it does not pause the statutory period. Confirm the legal trigger and deadline with the accountable privacy reviewer. Do not use an internal timer state as proof that an obligation was suspended, met, or excused.

Roles and decision authority

Name roles before the response expands. One person may hold more than one role in a small organization, but each authority should remain explicit. Avoid a large response group in which everyone can comment but no one owns the decision.

Incident lead: coordinates containment, investigation, dependencies, meeting cadence, and the integrated action list. The incident lead does not unilaterally decide the controller's regulatory position unless formally authorized and qualified to do so.

DPO or privacy decision owner: assesses the personal-data dimension, risk to rights and freedoms, notification requirements, data-subject communication, and professional-review needs. This owner records the rationale and any dissenting view.

Security or forensic lead: preserves technical evidence, controls access, tests containment, explains confidence and limitations, and separates confirmed findings from hypotheses. This role provides facts; it should not make unsupported legal conclusions.

Business or system owner: explains the processing purpose, affected workflow, data population, operational consequences, processor relationships, and safe recovery options. The owner confirms whether estimates are complete and current.

Communications owner: prepares clear regulator, data-subject, workforce, partner, or public communications only after the accountable decision and approval. Communications must not outrun verified facts or expose details that create more harm.

Management reviewer: accepts material residual business risk, resources remediation, resolves authority conflicts, and approves external positions within the organization's governance. Management review does not displace DPO independence or qualified advice.

Evidence coordinator: maintains a reference index, provenance, access restrictions, integrity notes, and decision links. This person does not copy sensitive evidence into the workbook merely to make it easier to circulate.

Client contributor: supplies only assigned facts or evidence through a scoped portal task. Contributors do not approve risk, decide whether notification is required, authorize external communication, or see internal deliberations beyond their assignment.

Create a short decision-rights statement: who may contain systems, who decides notification, who approves wording, who performs external delivery, who records proof, and who closes the incident. If authority is unavailable, escalate immediately to the named alternate rather than allowing the response to stall.

Stage 1 — Preserve facts and contain harm

Begin with reversible containment that reduces continuing exposure while preserving evidence. Security owners may isolate accounts, sessions, endpoints, integrations, credentials, or data flows according to the incident plan. Record the time, actor, reason, affected service, expected impact, and validation result for each significant containment action. Avoid destructive actions that would erase logs or prevent reconstruction unless immediate safety requires them and an authorized incident owner records why.

Establish a fact ledger with four states: confirmed, reported but unverified, estimated, and disproved. Each entry should identify its source and time. Keep raw logs, exports, images, malware samples, identity records, and affected datasets in the approved forensic or security repository. In Privora Pro, reference the evidence item and summarize its relevance; do not paste the underlying payload.

Ask what personal data may be involved, how confidentiality, integrity, or availability may have been affected, whether access continues, whether credentials or encryption keys are exposed, whether data could be combined with other available information, and whether a processor or recipient has parallel evidence. Identify vulnerable groups and immediate safety concerns early.

Containment and notification analysis run in parallel. A team should not delay risk assessment until every root-cause question is answered. Equally, urgency does not justify publishing guesses as facts. Use bounded estimates, record confidence, and schedule the next fact review.

The stage output is a contained or explicitly uncontrolled incident state, a preserved evidence index, a current fact ledger, and a list of urgent harm-reduction actions. Escalate if containment would create material safety, legal, service, or evidence-preservation risk.

Stage 2 — Start the incident clock and assign owners

Verify the awareness time with the privacy decision owner and record the reasoning. Use the Privora Pro breach detail to monitor elapsed time and the compliance calendar to keep review points visible. The timer is not a legal conclusion. If it was started late, paused, or resumed, preserve the true awareness record and explain the operational discrepancy rather than changing facts to match the display.

Set review points based on the remaining time and uncertainty. A practical cadence may include an immediate triage, a fact and risk review, a notice-readiness review, and a final authority check. These are internal controls, not new statutory windows. Shorten the cadence if harm continues or confidence is low.

Assign every action to a named owner with a due time, dependency, status, and escalation path. Distinguish the person doing the work from the person accountable for approving the result. Assign alternates for the DPO, incident lead, security lead, communications owner, and filing operator. Confirm availability across time zones and outside normal working hours.

Record processor notifications, insurance or counsel contacts, contractual notices, and sector questions as separate work items. Do not assume that the general statutory rule resolves a contract or sector duty.

This kit includes no shorter sector deadline because none is registered as a current authoritative source for this release. Obtain qualified review where another duty may apply.

The stage output is an accepted awareness time, operational deadline view, response roster, action register, decision calendar, and escalation chain. A missed internal review point triggers escalation; it does not automatically answer whether the external obligation was met.

Stage 3 — Establish affected people, data, systems, and processors

Build the best available impact picture without circulating affected records. Identify the processing activity, systems, environments, locations, processors, sub-processors, recipients, and interfaces involved. Separate confirmed scope from the maximum credible scope. Record the query or method used to produce each count and the time at which the estimate was generated.

Describe affected people by relevant category, such as customers, workers, children, patients, applicants, or business contacts. Note vulnerability factors without adding unnecessary personal detail. Estimate the number of people and records using ranges when exact counts are not yet reliable. Explain possible duplication, stale records, shared accounts, logging gaps, or inaccessible systems.

Classify data by sensitivity and practical misuse potential. Consider identity and contact data, financial details, authentication material, communications, location, health, biometric, employment, children's data, and combinations that make profiling or fraud easier. Do not reduce the analysis to a checklist: the context, protection state, exposure mechanism, and ability to identify people matter.

For each processor, record the contract owner, notice time, information received, required follow-up, preservation request, and whether the processor can support affected-population estimates. A processor contribution informs the controller; it does not transfer the controller's decision authority.

Reconcile conflicting estimates explicitly. Name the preferred estimate, alternative, reason for difference, owner, and next update. The stage output is a versioned scope statement with affected categories, approximate counts, data categories, systems, processor involvement, limitations, and evidence references.

Stage 4 — Assess risk to rights and freedoms

Assess how the breach could affect individuals, not only how costly it is to the organization. Consider fraud, identity theft, discrimination, financial loss, physical or psychological harm, loss of confidentiality, loss of control, safety risks, exclusion, reputational harm, and exposure of sensitive relationships or activity. Consider severity and likelihood separately, then explain the combined judgment.

Evaluate the nature and volume of data, ease of identification, protection measures, whether keys or credentials are compromised, exposure duration, recipient trustworthiness, evidence of access or misuse, reversibility, vulnerability of affected people, and the effectiveness of containment. Encryption or deletion may reduce risk only if the team can support that conclusion with facts.

Record at least two perspectives where uncertainty is material: the current evidence-based view and the credible adverse view. Identify assumptions that would change the notification decision. Ask security, privacy, business, and DPO reviewers to state disagreements rather than smoothing them into a vague consensus.

Classify the controller-notification question around whether the breach is likely to result in a risk to rights and freedoms. Classify the data-subject communication question separately around high risk. A decision on one does not automatically decide the other. Record the evidence, rationale, reviewer, date, and next reassessment trigger.

Use professional review for close calls, vulnerable populations, large or uncertain scope, sensitive data, continuing exposure, conflicting evidence, or potential sector duties. The stage output is a signed risk decision record with confidence, assumptions, dissent, mitigation effect, and review trigger.

Stage 5 — Make and record notification decisions

The privacy decision owner records a separate decision for the Commission and for affected data subjects. For the Commission, state whether the breach is likely to result in risk, what evidence supports the conclusion, when awareness occurred, the 72-hour point, who approved the position, and who will

deliver the notice if required. If the decision is not to notify, preserve the reasoning and schedule reassessment if facts change.

For high-risk effects, record whether immediate communication to affected data subjects is required, the audience, practical protective steps, language and accessibility needs, feasible delivery methods, and any reason direct communication is not feasible. Obtain qualified review before relying on an alternative public communication.

When notification is required but details are incomplete, prepare the known information and a phased-update plan. Identify each missing element, owner, expected availability, and how the follow-up will be sent without undue delay. Do not delay the initial decision simply to make the first notice look complete.

Use Privora Pro to maintain the decision, supporting facts, draft notification plan, and external reference after one is received. Generating a notice creates material for professional review. The authorized operator must deliver it through the current approved external channel and retain independent proof of delivery.

> **Authorize the external position**
> Before external delivery, confirm the factual owner, privacy reviewer, approver, delivery operator, recipient/channel, version, and evidence of authorization. A generated document or Mark Submitted status is not proof of external receipt.

The stage output is a dated, approved notification decision for each audience, a version-controlled notice if required, a delivery owner, and a follow-up schedule.

Stage 6 — Prepare communications and preserve evidence

Prepare communications from the approved fact set. Regulator material should clearly identify the controller and contact point, describe the circumstances and nature of the breach, state the relevant dates, categories and approximate numbers where feasible, likely consequences, measures taken or proposed, risk assessment, and outstanding phased information. Do not imply certainty where an estimate remains under review.

Data-subject communication should be plain, specific, accessible, and action-oriented. Explain what happened, what information is involved, likely consequences, what the organization has done, what the person can do, where to obtain help, and how updates will be provided. Avoid technical detail that enables further abuse or defensive language that obscures practical protection.

Coordinate workforce, processor, customer-service, media, insurer, law-enforcement, and partner messages without collapsing their purposes. Each communication needs an audience, owner, approved version, delivery time, channel, and proof. Confirm that support teams can answer likely questions and escalate vulnerable-person needs.

Preserve every issued version and delivery record. In the Privora record, link the approved document and note the external delivery evidence. Do not store recipient lists or sensitive response material in this runbook. Keep those records in the authorized communication or case system and reference them safely.

The stage output is an approved communication pack, recipient/channel plan, support briefing, delivery evidence register, and update cadence. Escalate any conflict between speed, accuracy, safety, or authority to the incident lead and DPO.

Stage 7 — Track remediation and residual risk

Move from containment to durable correction. Separate immediate containment, recovery, root-cause correction, control improvement, monitoring, data-subject support, processor action, and governance changes. Each remediation item needs an accountable owner, completion evidence, target date, dependency, validation method, and residual-risk reviewer.

Do not close an action because a ticket says complete. Review evidence that the change was implemented and effective. For technical controls, record the validation result and period. For process

changes, record approval, communication, training, or sampling evidence. For processor actions, retain the response and controller review.

Monitor for misuse, recurrence, failed recovery, delayed communications, new affected populations, and facts that change the notification analysis. Reopen the decision when a trigger occurs. Record any additional notice or correction and link it to the original position.

Management accepts residual business risk only after the DPO or privacy owner can explain the rights-and-freedoms implications. Acceptance should not be used to erase open work. Mark blocked items, name the blocker, escalate resources, and keep the next review date visible in deliverables and the calendar.

The stage output is a reviewed remediation register, validated containment, residual-risk decision, monitoring plan, and linked evidence. Open remediation may continue after incident closure only when ownership, deadlines, escalation, and review remain active.

Stage 8 — Close with a post-incident review

Close the response when the incident state is stable, required decisions and communications are completed or explicitly tracked, evidence is preserved, residual risk is accepted by the proper authority, and remaining remediation has durable ownership. Closure is a governance decision, not the moment the 72-hour timer stops.

Run a blameless but accountable post-incident review. Compare the actual awareness path, escalation, containment, evidence quality, decision timing, communication, processor response, and recovery with the intended process. Identify control failures and response-system failures separately. Record what helped, what delayed work, what evidence was unavailable, and what would reduce harm or uncertainty next time.

Confirm that the Privora record contains the approved summary, decision rationale, activity history, notice status, external reference where received, remediation links, and closure review. Check that sensitive source material remains in the proper repository and that access can be reduced after the emergency.

Assign lessons to owners with review dates. Feed relevant actions into training, vendor review, DPIA review, retention design, access control, incident exercises, or the next quarterly client review. Do not publish invented success metrics. Report only observed facts with a defined source, period, and reviewer.

The stage output is a closure decision, post-incident review, lessons register, open-action handoff, and next review date.

Late, incomplete, and processor notifications

If the response is late, preserve the true awareness and action timeline. Escalate immediately, obtain qualified review, prepare the best available notice if required, and record the reasons for delay. Do not alter timestamps, restart an operational timer, or describe an internal pause as suspending the statutory period.

If information is incomplete, identify what is known, the limits of each estimate, why information is unavailable, the person resolving it, and the phased-update plan. Under section 40, information that cannot be provided at the same time may be provided in phases without undue delay. Keep each update version and delivery evidence linked to the incident.

If a processor reports the breach, record when it became aware, when it informed the controller, the facts supplied, the preservation steps taken, and outstanding requests. The controller should make its own documented risk and notification decisions. Escalate poor processor cooperation through the contract owner and professional reviewer.

If new facts reverse an earlier decision, record the prior basis, new evidence, revised decision, approval, and corrective communication. A changed decision is not a reason to erase history; the sequence is part of the defensible operating record.

Completion criteria

Complete the active response only when:

- awareness, incident, discovery, and material action times are recorded with sources;

- response roles, authority, alternates, and escalation paths are clear;
- containment is validated or the uncontrolled risk is explicitly escalated;
- the affected population, data, systems, processors, estimates, and limitations are documented;
- risk to rights and freedoms and high-risk effects have separate reviewed decisions;
- Commission and data-subject notification decisions have rationale and approval;
- required communications have approved versions and independent delivery evidence;
- the Privora status is reconciled with external reality and does not stand in for filing proof;
- remediation and monitoring have owners, dates, evidence, and residual-risk review;
- sensitive source material remains in approved systems with restricted access;
- closure and lessons are approved, and open work is handed into durable tracking.

The DPO or privacy decision owner should sign the completion review. Where facts or duties remain contested, mark the record incomplete and escalate rather than declaring a clean closure.

Record the work in Privora Pro

Use the client breach register to create and review the incident record. Use the breach detail for awareness context, affected estimates, impact assessment, containment summary, notification plan, activity history, generated notice review, and the manual status that reflects verified external action. Use the calendar and deliverables for time-bound reviews and remediation follow-up.

Open the client breach register · Privora Pro console

Continue the breach record · Privora Pro console

Review response deadlines

Record only approved summaries and references appropriate to the workspace. Verify tenant and client context before every action. Treat generated notices as drafts until reviewed and approved. Confirm external delivery independently, then record the accurate status and reference. Preserve corrections rather than overwriting the decision history.

Sources and professional review

Regulatory content was reviewed on 12 August 2026 against the official local copies of the Nigeria Data Protection Act 2023, section 40, and the Nigeria Data Protection Commission General Application and Implementation Directive 2025, article 33. Recheck current authoritative material at the time of an incident because law, guidance, channels, and sector duties can change.

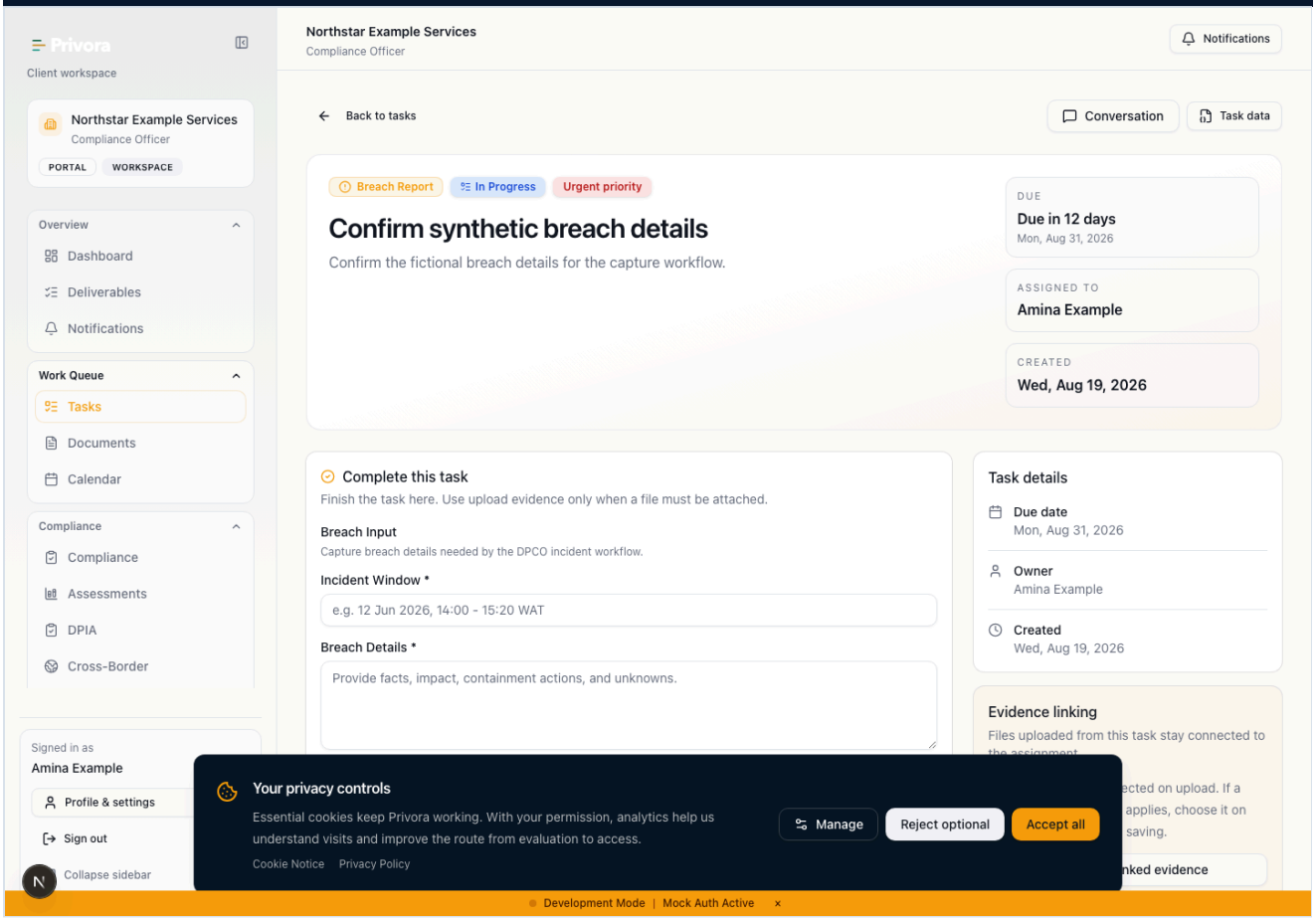
Section 40, especially subsections (1)–(4), (8), and (9)

Article 33, especially paragraphs (1)–(5)

Implemented breach register, timer, calendar, generated-document review, portal task, and activity behavior

Privacy Operations category and professional-judgment boundaries

Obtain professional review for notification thresholds, vulnerable populations, incomplete or disputed facts, public communication, contracts, cross-border implications, law-enforcement interaction, litigation privilege, and any sector obligation. This guide organizes work; accountable professionals decide and act.



Use the Portal breach task view to continue the privacy operations workflow.
1. Breach task heading

Complete an assigned breach contribution

Use only the portal task assigned by the DPCO or privacy team. Read the requested question, acceptance criteria, due time, and permitted evidence type. Provide a concise factual answer: what you observed, when it occurred, which system or process you own, how the fact was verified, and where the approved evidence is retained. Use estimates only when labelled with their method, time, and limitation.

Do not paste raw incident payloads, credentials, full affected-person lists, forensic images, or copied sensitive records into comments. Upload or reference evidence only as the task and your organization's secure handling procedure allow. Ask the engagement owner for clarification when the request is broader than your authority or would expose unnecessary personal data.

Contributors provide assigned facts or evidence; they do not decide risk, approve a notice, or submit it to the Commission. After submission, the privacy team reviews sufficiency, may return the contribution for clarification, and keeps decision authority.

Open the assigned portal task · Privora Pro client portal