Privora

PRIVACY OPERATIONS · PRIVORA PRO · RUNBOOK

Run a DPIA as an accountable operating workflow

Run one staged assessment with named contributors, accountable treatment owners, explicit decision gates, and retained review history.

Primary action

Start the DPIA workflow 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 DPIA as an accountable operating workflow

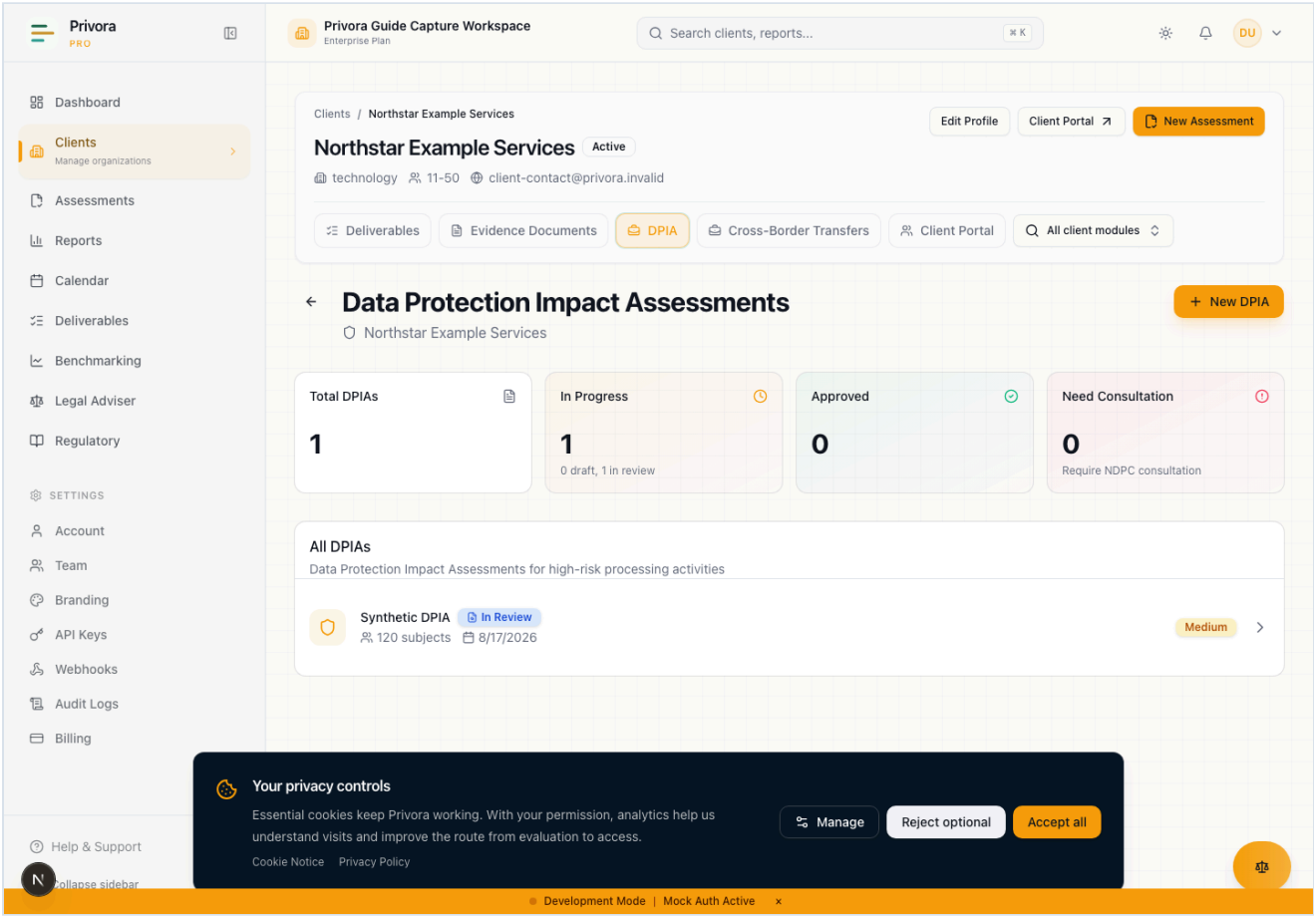
> Operational guidance — not legal advice. This guide does not guarantee compliance.

Apply this method with qualified privacy, legal, security, and sector review. A blank copy may be shared for planning, but completed material may be confidential. Keep personal data, security detail, consultation records, and evidence in the authorised Privora Pro workspace rather than email or this runbook. Privora Pro remains the operating record after reviewed information is entered.

The operating outcome

Product walkthrough

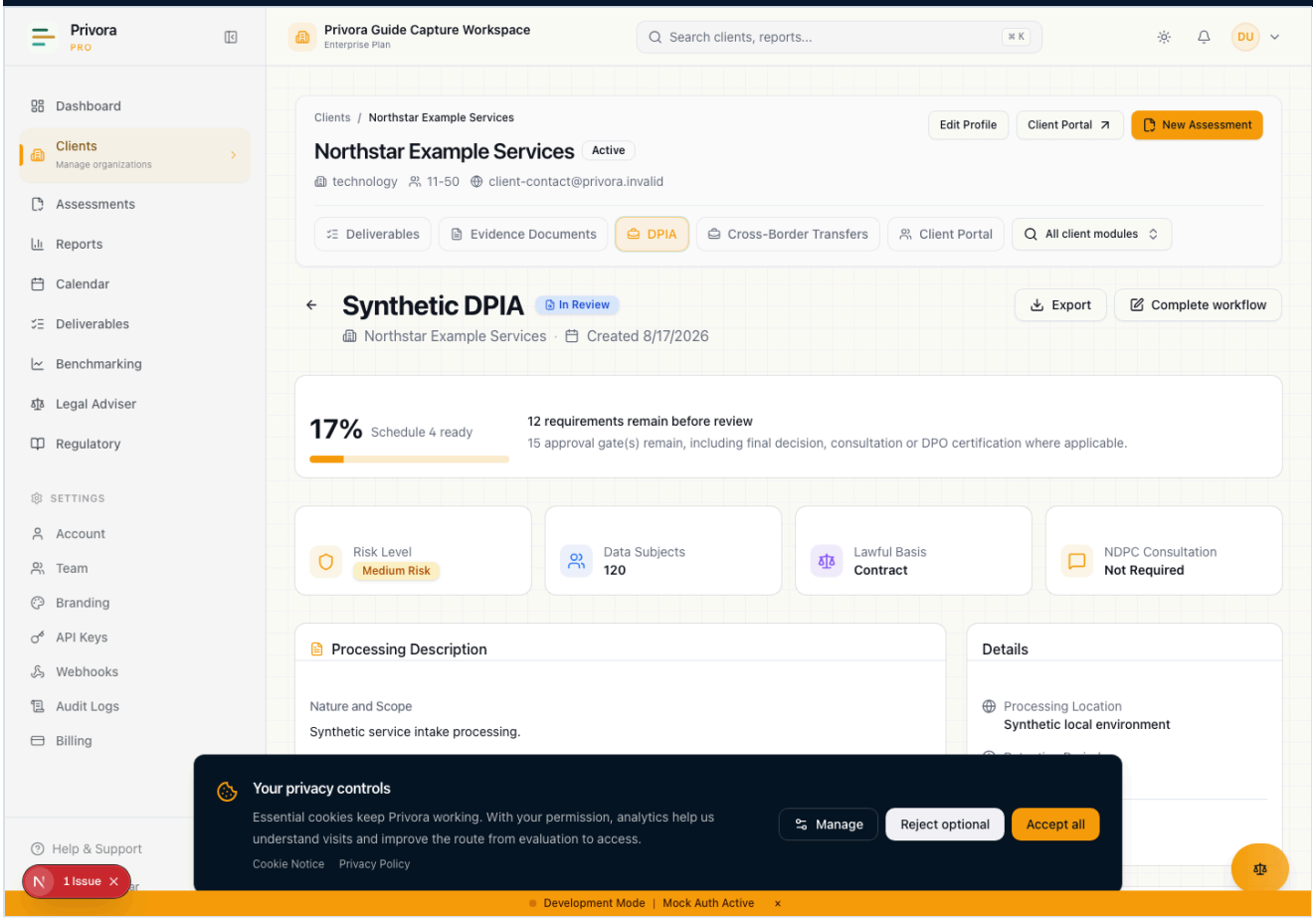
Open the client workspace, choose DPIA, and use the assessment detail page to move from screening to review. When a contributor is needed, assign the portal task from the assessment workflow and use the returned contribution as review input rather than as approval.



Use the Console dpia list view to continue the privacy operations workflow.
1. DPIA heading

How to reach this page

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



Use the Console dpia detail view to continue the privacy operations workflow.
1. DPIA title

A data privacy impact assessment is useful when it changes how a team decides. The outcome is not a completed questionnaire. It is a traceable record showing why an assessment began, what processing is proposed, whose rights may be affected, which evidence was reviewed, who owns treatment, whether prior consultation is required, and who has authority to approve the result.

This runbook is for Nigerian DPCOs, in-house DPOs, privacy leads, business owners, security owners, and certified DPO reviewers. It improves the recurring workflow from a high-risk trigger to a maintained decision. It is better than a document-only approach because facts, contributions, risk treatment, decisions, and history remain connected. It reduces operational complexity by giving each role one stage, one output, and one next action.

Use Privora Pro to preserve the current assessment, portal tasks, treatment ownership, status, report, and activity history. Use professional judgment to interpret the law and the facts. System validation can show that fields or gates are incomplete; it cannot decide that processing is lawful, necessary, proportionate, or acceptable.

When a DPIA workflow begins

Begin before processing where the proposed nature, scope, context, or purpose may create high risk to a data subject's rights and freedoms. Screen planned work, pilots, material changes to existing processing, new technology, systematic monitoring, sensitive data, vulnerable people, automated decisions, large-scale processing, public surveillance, and cross-border transfers. Do not wait for procurement, build, or launch to make the decision irreversible.

An existing activity also needs a fresh screen when its purpose, data categories, population, recipients, technology, location, retention, control environment, or risk changes. Reopening an approved assessment creates a new version in the implemented workflow and clears the previous sign-off. This preserves the earlier decision without treating it as approval of the changed activity.

Record the processing stage as planned, pilot, or ongoing. State the trigger and rationale in plain language. If the team concludes that a DPIA is not required, preserve that reason through the

organisation's approved decision process; do not create a false high-risk assessment merely to satisfy a template.

The Nigeria Data Protection Act 2023, section 28(1), places the assessment before likely high-risk processing. Section 28(2) places consultation with the Nigeria Data Protection Commission before processing where envisaged measures do not remove the high risk. These are sequencing controls, not labels to add after launch.

Section 28(1)–(2), official PDF p. A735

Roles and authority boundaries

Name roles before collecting evidence. One person may hold more than one role in a small team, but the authority must remain explicit.

Role	Accountable work	Authority boundary
Privacy lead or DPCO consultant	Scope the assessment, evaluate contributions, analyse rights impact, coordinate treatment, and prepare the decision	Does not impersonate the certified DPO or the Commission
Business or system owner	Explain purpose, operations, systems, data flows, recipients, retention, and proposed changes	Supplies facts; does not set the formal risk conclusion
Security or control owner	Explain vulnerabilities, control design, operation, evidence, gaps, and remediation	Supplies technical assessment; does not approve the processing decision
Management reviewer	Recommend go ahead, modify, or stop with conditions and resources	Recommendation does not replace privacy assessment or certified-DPO vetting
Certified DPO	Vet the completed assessment, challenge gaps, attest, approve, reject, or require changes within the controlled console workflow	Cannot bypass unresolved high-risk prior consultation
NDPC	Exercises external regulatory authority and receives consultation or required submissions through authorised channels	Privora has no regulator account or regulator API integration

Contributors work through scoped portal tasks. Their submissions are evidence for evaluation. They do not silently overwrite the formal DPIA, change risk ratings, record an NDPC outcome, certify a DPO review, or approve processing. The privacy lead remains accountable for reconciliation, and the certified DPO remains accountable for the vetting decision.

Use least privilege. Confirm tenant and client before assigning a task, and give a contributor only the facts needed for the request. Do not expose internal deliberation or unrelated client information merely because someone can contribute to one stage.

Stage 1 — Screen the trigger and timing

Owner: privacy lead. Inputs: project brief, change request, processing inventory, system proposal, and initial stakeholder list. Output: recorded trigger screen and timing rationale.

Meet the sponsor early. Ask what decision is still open, what happens if the activity is delayed or changed, and which personal-data use creates concern. Select every relevant trigger rather than choosing only the easiest category. Explain the connection between the trigger and possible rights impact. Record the processing stage and the date by which the assessment must inform the decision.

Check whether procurement, vendor onboarding, product design, policy approval, or deployment has already created a commitment. Escalate if commercial timing is being used to compress assessment. A DPIA completed after the decision can document risk, but it cannot retroactively satisfy a before-processing sequence.

Decision point: if likely high risk is present, continue and keep processing behind the agreed gate. If the evidence is incomplete, assign fact-finding before deciding. If the activity is outside scope, record the screening outcome under the organisation's reviewed method.

Record in Privora Pro: create the DPIA under the correct client, capture triggers, processing stage, and rationale, and assign the privacy lead. The application records the workflow; the operator supplies the judgment.

Stage 2 — Define scope and data flow

Owner: privacy lead with business and system owners. Inputs: architecture, process map, contracts, notices, records of processing, retention rules, and vendor facts. Output: one agreed processing description.

Describe the nature, scope, context, and purpose in terms a reviewer outside the project can understand. Record whether operations are automated, manual, or mixed. Identify personal and sensitive categories, affected groups, approximate scale, sources, collection points, uses, storage, access roles, recipients, processors, transfers, retention, deletion, and hosting or processing locations.

Draw the flow from collection to deletion. Separate facts from assumptions and identify the owner of every unresolved fact. For each third party, record its purpose, location, processor relationship, contract state, and transfer basis where relevant. State the intended scope and the controls that should detect scope creep.

Complete the corresponding Schedule 4 adequacy ratios only after the supporting narrative exists. A score without evidence is not a finding. Where teams disagree, retain the disagreement and escalation rather than averaging views into false certainty.

Record in Privora Pro: enter the processing description, purpose, categories, population, retention, location, recipients, material information, operation type, third-party assessment, and scope-creep controls. Link supporting evidence in the authorised workspace, not in an email attachment chain.

Stage 3 — Assess lawful basis, necessity, and proportionality

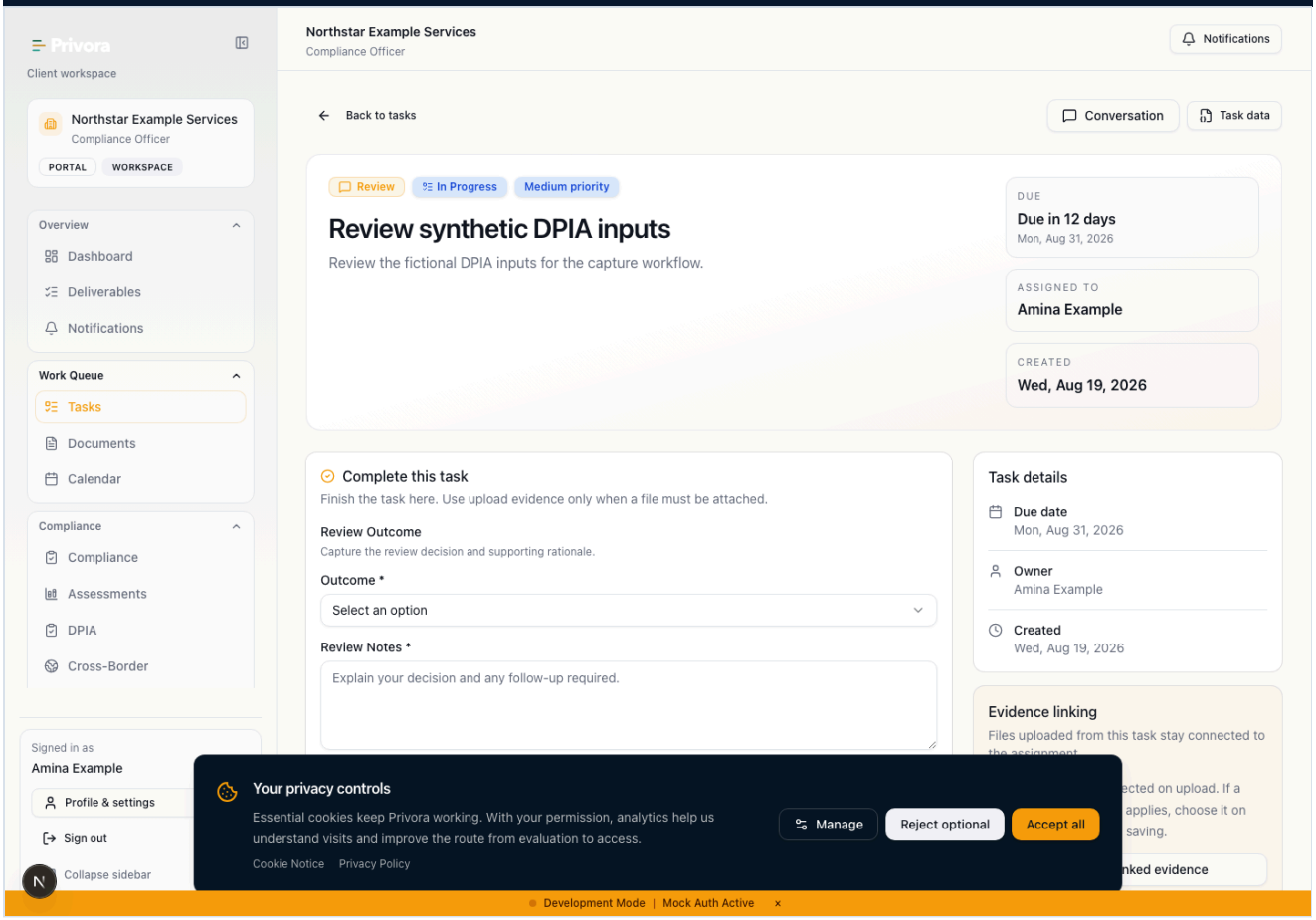
Owner: privacy lead with qualified legal or privacy review. Inputs: stated purpose, lawful-basis analysis, alternatives, notices, contracts, and policy authority. Output: documented assessment, not a dropdown alone.

Select the claimed lawful basis and explain why it applies to each material purpose. Check whether sensitive-data conditions, children's data, employment context, or sector obligations require additional analysis. Do not treat consent as a convenient default or infer that a product requirement makes processing necessary.

Test necessity by asking whether the purpose can be achieved without the personal data, with fewer fields, at lower precision, for a smaller population, or for a shorter time. Test proportionality by comparing expected benefit with intrusion, power imbalance, vulnerability, discrimination, exclusion, chilling effects, loss of control, and the ability to exercise rights.

Document less intrusive alternatives and why each was accepted or rejected. If the alternative analysis changes the design, return to scope and data flow. If there is no defensible basis or proportionate design, the correct result may be modify or stop.

Record in Privora Pro: preserve the basis, rationale, necessity assessment, proportionality assessment, alternatives, and supporting section score. A completed field is a record of analysis, not an automatic legal conclusion.



Use the Portal dpia task view to continue the privacy operations workflow.
1. DPIA task heading

Stage 4 — Collect scoped portal contributions

The privacy lead may request processing context, stakeholder observations, control evidence, or a management recommendation from an active client contributor. Define the question, acceptance criteria, due date, and safe evidence location. Ask only for facts within that person's role.

If you receive an assigned task, answer the specific question, identify the period and system covered, state what you know, distinguish assumptions, and reference evidence already stored in the authorised workspace. Do not place passwords, secrets, raw sensitive data, full identity records, or unnecessary security detail in comments. Ask the engagement owner when the request is unclear.

Submitting a contribution does not grant risk-rating, consultation, approval, certified-DPO, delivery, or final decision authority. The privacy team reviews the contribution, may return it for clarification, and decides how it affects the assessment. A management recommendation remains a recommendation.

Open assigned DPIA contribution task · Privora Pro client portal

Stage 5 — Analyse vulnerability and rights impact

Owner: privacy lead with security and relevant subject-matter owners. Inputs: data flow, threat and control evidence, stakeholder findings, and affected-group context. Output: rights-centred vulnerability analysis.

Assess confidentiality, integrity, and availability, but do not stop at security. Consider the effect on people if data is inaccurate, unavailable, disclosed, combined, inferred, retained, or used beyond expectation. Examine vulnerability arising from age, disability, health, employment power, financial dependency, immigration status, digital exclusion, or limited ability to challenge a decision.

Describe likely impacts such as discrimination, denial of service, economic loss, reputational harm, surveillance, loss of autonomy, physical risk, or inability to exercise a right. Record disparate outcomes

and whether some groups bear more risk than others. Evaluate remediation speed, disaster-recovery implications, and the technical capacity of people operating controls.

Use evidence that is current and specific. A policy saying encryption is required is not evidence that the relevant store is encrypted. A penetration test may support security findings but does not answer fairness, necessity, or rights questions.

Record in Privora Pro: capture stakeholder findings or the reason consultation was not appropriate, CIA impacts, identified vulnerabilities, data-subject vulnerability and impact, remediation capability, technical capacity, disparate outcomes, and principles-and-rights analysis.

Stage 6 — Assign accountable risk treatment

Owner: privacy lead; each treatment has a named accountable owner. Inputs: identified rights risks, existing controls, design alternatives, and control evidence. Output: owned treatment plan with residual ratings.

Write each risk as a cause, event, and effect on people. Record likelihood and severity using the adopted Schedule 4 scale. Identify existing and planned mitigations, the owner, target date, status, evidence, and unresolved-risk plan. Do not use a team name where no individual is answerable.

Assess residual risk after the measure, not after the promise to implement it. If evidence is missing, treat the control as unverified. Where a risk is accepted, name the authorised decision-maker and rationale; contributor agreement is not risk acceptance.

Review how controls interact. A control that reduces fraud may increase exclusion or identity collection. A security measure may create availability risk. Privacy by design and default should reduce collection, access, exposure, retention, and dependence on later remediation.

Decision point: high or very-high residual risk activates the prior-consultation path. Do not lower a rating to avoid the gate. Record in Privora Pro: maintain the risk register, controls, owners, dates, treatment status, residual risk, privacy-by-design measures, and minimum necessary measures.

Stage 7 — Assess transfers and rights implications

Owner: privacy lead with transfer and legal specialists where required. Inputs: recipient and location map, transfer assessment, safeguards, redress paths, and rights process. Output: completed transfer and rights analysis.

When processing crosses borders or makes data available from another jurisdiction, identify countries, recipients, purpose, legal basis, safeguards, onward transfers, and realistic redress. Consider sovereignty, security, discrimination, and other applicable law. Do not infer that a vendor contract alone resolves transfer risk.

Test how people receive information, access data, request correction or erasure, object, restrict processing, challenge automated decisions, and use any portability right that applies. Consider authentication, accessibility, language, channel, and the risk of disclosing information to the wrong person. Explain how rights requests reach an accountable owner and how unresolved restrictions receive qualified review.

If no transfer applies, state the evidence for that conclusion. If rights cannot be supported as designed, return to treatment or modify the processing.

Record in Privora Pro: complete jurisdictions, transfer basis, safeguards, rights and redress, discrimination risk, sovereignty and security, applicable law, and the section score. Keep legal conclusions subject to qualified review.

Stage 8 — Record go, modify, or stop

Owner: authorised management reviewer informed by the privacy assessment. Inputs: readiness checklist, risks, treatment, consultation status, unresolved issues, and recommended conditions. Output: explicit operational decision and rationale.

Choose go ahead only when the evidence and measures support proceeding within recorded conditions. Choose modify where design, controls, scope, timing, or ownership must change. Choose stop where the

purpose is unnecessary, disproportionate, unsupported, or cannot be made acceptable. A stop decision cannot be converted into permission to process by completing a sign-off field.

Record conditions, dependencies, unresolved problems, sandbox recommendation, minimum measures, review frequency, and the event that should trigger an earlier review. State who monitors each condition. Keep commercial preference separate from the rights-risk conclusion.

The assessment may remain a draft while evidence or treatment is incomplete. In-review status signals formal challenge, not approval. Only the controlled approval path produces an approved record. Make the draft/approved distinction visible when sharing a report.

Record in Privora Pro: select the final decision, enter rationale and review plan, and resolve readiness blockers before seeking sign-off.

Stage 9 — Complete prior consultation where required

Owner: privacy lead coordinating an externally authorised process. Inputs: completed DPIA, high residual-risk basis, measures considered, questions, and approved submission material. Output: retained consultation record and outcome.

Where the assessment indicates high risk remains notwithstanding envisaged measures, section 28(2) requires consultation with the Commission before processing. Pause the decision gate. Prepare a reviewed assessment, explain unresolved risk, and follow the organisation's authorised regulatory process. Record the consultation date, outcome, and authentic reference only after they exist.

Privora Pro does not submit the DPIA, connect to an NDPC account, or produce a filing receipt. A status or reference field is an internal operating record, not evidence of regulator acceptance. Do not use fictional references outside a clearly labelled demo.

GAID Article 28 contains additional filing, timing, certified-DPO, privacy-by-design, and Schedule 4 provisions. Their application to the facts needs qualified review, particularly where transitional dates or submission duties are involved.

Section 28(2), official PDF p. A735

Stage 10 — Obtain certified DPO vetting

Owner: certified DPO. Inputs: complete assessment, evidence index, decision, consultation outcome where required, and unresolved exceptions. Output: vetted decision, comments, attestation, and controlled sign-off.

The certified DPO reviews scope, source quality, necessity, proportionality, affected groups, risks, treatment, residual risk, consultation, and the final decision. The reviewer may approve, reject, or return the record with required changes. Record certification identifier, review date, comments, explicit attestation, and sign-off through the console.

The application record is not a cryptographic or legally qualified signature. It does not prove identity beyond the product's authenticated workflow. Stronger signature or identity assurance, if needed for a submission or sector process, must be handled through an approved external method.

Portal users cannot perform this action. The privacy lead cannot use a contributor's recommendation as DPO vetting. High residual risk cannot bypass the consultation gate.

Article 28(4), (11)–(13), official PDF printed pp. 33–34

Stage 11 — Report, retain history, and review

Owner: privacy lead with records and management owners. Inputs: vetted assessment and approved supporting record. Output: controlled report, retained history, and scheduled review.

Generate the report from the current Privora record. Check title, version, status, scope, ratios, treatment, consultation, decision, and sign-off before distribution. Draft output must remain visibly draft. An approved export records the product workflow state; it does not claim NDPC approval or replace any separately authorised submission.

Retain activities showing contributions, changes, returns, consultation, decision, and sign-off. Limit distribution according to confidentiality and need to know. Link approved results to related governance or

reporting work where the organisation requires it.

Set a review cadence proportionate to change and risk. The implemented workflow supports monthly, bimonthly, quarterly, biannual, annual, biennial, lifecycle, or custom review. Calendar cadence never replaces event-driven review. Reopen when purpose, data, people, scale, technology, recipients, location, control effectiveness, incident history, or law changes.

Record in Privora Pro: generate the current report, confirm status, retain the activity history, and monitor the next review. Privora Pro remains the operating record; exported documents are controlled views of that record.

Exceptions and escalation

Escalate immediately when processing starts before the assessment, scope is disputed, evidence is unavailable, an owner refuses treatment, a vulnerable group may face serious harm, residual risk remains high, a contributor exceeds authority, or a consultation or DPO record appears unreliable.

Do not solve missing evidence by weakening a statement. Record the gap, owner, effect, interim restriction, and next review date. Pause processing where the approved governance process requires it. If commercial deadlines conflict with risk treatment, send the decision to the named management and privacy authorities with the trade-off visible.

Correct cross-client assignments and access issues before continuing. Do not copy sensitive material into this runbook. Where a regulatory interpretation, sector rule, submission duty, or signature requirement is uncertain, obtain qualified advice and retain the reviewed conclusion with its date and source.

Completion criteria

The workflow is complete for the current version only when:

- the trigger, timing, scope, data flow, population, retention, locations, recipients, and purpose are reviewable;
- lawful basis, necessity, proportionality, alternatives, vulnerabilities, rights, transfers, and disparate outcomes are assessed;
- contributions have been evaluated rather than copied into findings;
- every material risk has treatment, an accountable owner, status, evidence expectation, and residual rating;
- the go ahead, modify, or stop decision has rationale and conditions;
- required prior consultation has an authentic date, outcome, and reference;
- certified-DPO vetting and application attestation are complete without overstating signature assurance;
- draft and approved outputs are distinguishable;
- activity history and the next review trigger are retained; and
- exceptions are resolved, accepted by authorised owners, or visibly carried forward.

Completion supports review readiness and does not remove the need to revisit the assessment when facts change.

Sources and professional review

Regulatory statements were reviewed on 12 August 2026 against the official local Nigeria Data Protection Act 2023 PDF, section 28, and the official NDPC General Application and Implementation Directive 2025 PDF, Article 28. Product instructions were checked against the current Privora Pro DPIA and portal workflow source. Brand instructions follow Privora's Privacy Operations positioning.

Section 28(1)–(4), official PDF p. A735

Article 28(1)–(13), official PDF printed pp. 31–34

Implemented DPIA workflow, portal contribution, report, history, and route contracts; reviewed 2026-08-12

Rules and regulatory practice can change. Confirm the current official material, sector obligations, submission method, certified-DPO requirements, and organisation-specific authority before acting.