PRIVACY OPERATIONS · PRIVORA PRO · RUNBOOK

Run an accountable evidence request and review cycle

Run one traceable Request to Report cycle with acceptance criteria, an accountable owner, contextual submission, human review, decision, and reporting link.

Primary action

Start an accountable evidence request 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 an accountable evidence request and review cycle

This runbook helps Nigerian DPCOs, in-house DPOs, evidence reviewers, and client contributors move evidence through one accountable operating sequence: Request → Owner → Evidence → Review → Decision → Report. It is designed for recurring Privacy Operations work where the team must preserve purpose, ownership, version context, review rationale, and the link to a requirement or client output.

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

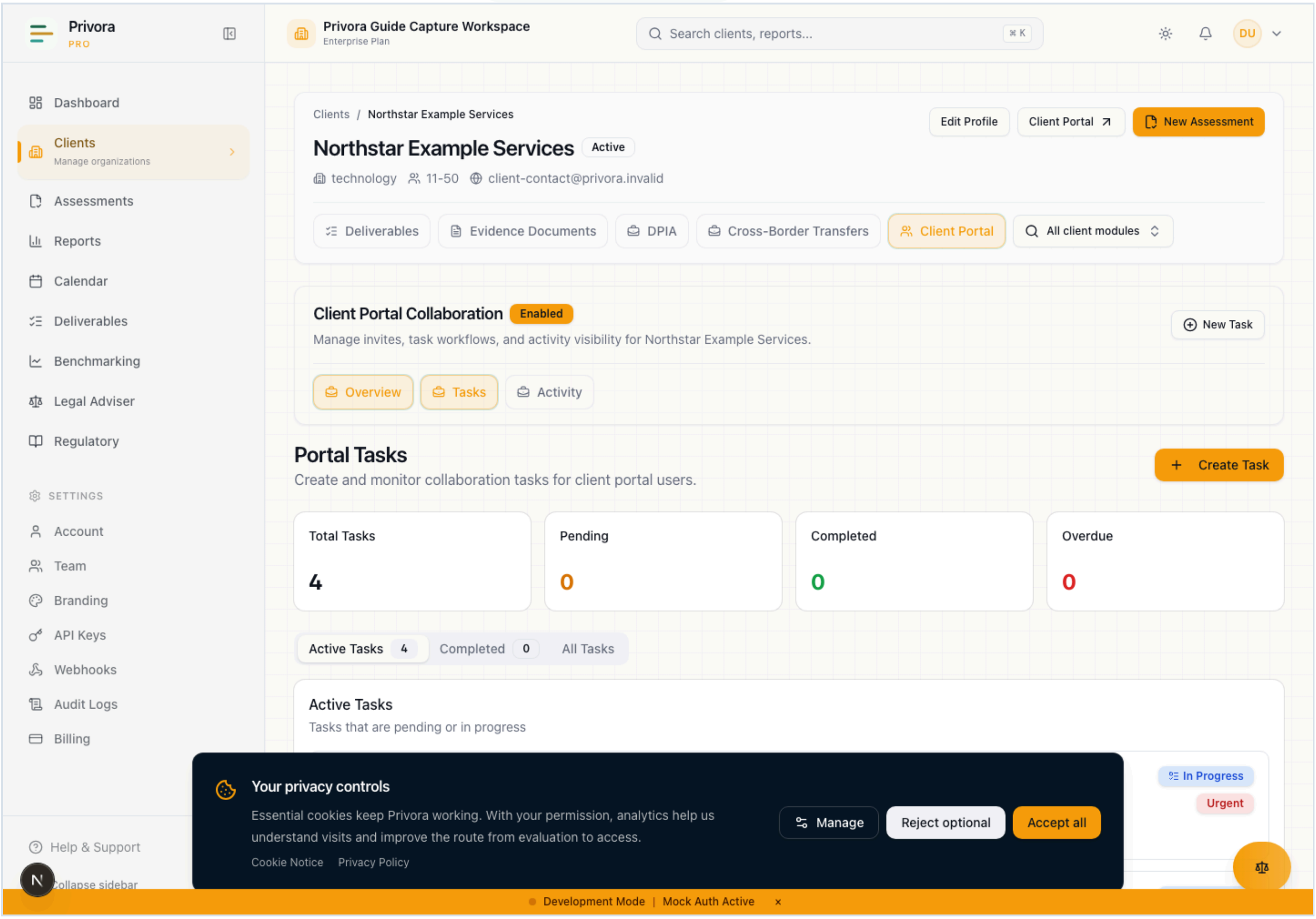
Apply qualified professional judgment to legal interpretation, regulatory conclusions, privilege, risk, and client-specific decisions. Privora Pro structures the workflow and history; it does not decide whether evidence proves compliance.

Store sensitive operational records only in authorized systems. Use the workbook for safe preparation and Privora Pro for approved tasks, documents, review outcomes, decisions, and reporting links. Confirm the correct organization and client before requesting, uploading, viewing, or reviewing evidence.

Console operator path

Product walkthrough

Open the client workspace from the Console dashboard, then use Portal Tasks to create or review the request. Use the task detail view to confirm ownership and context, Documents to review the submitted record, and Deliverables to connect the approved result. These screenshots show the order without exposing client or task identifiers.

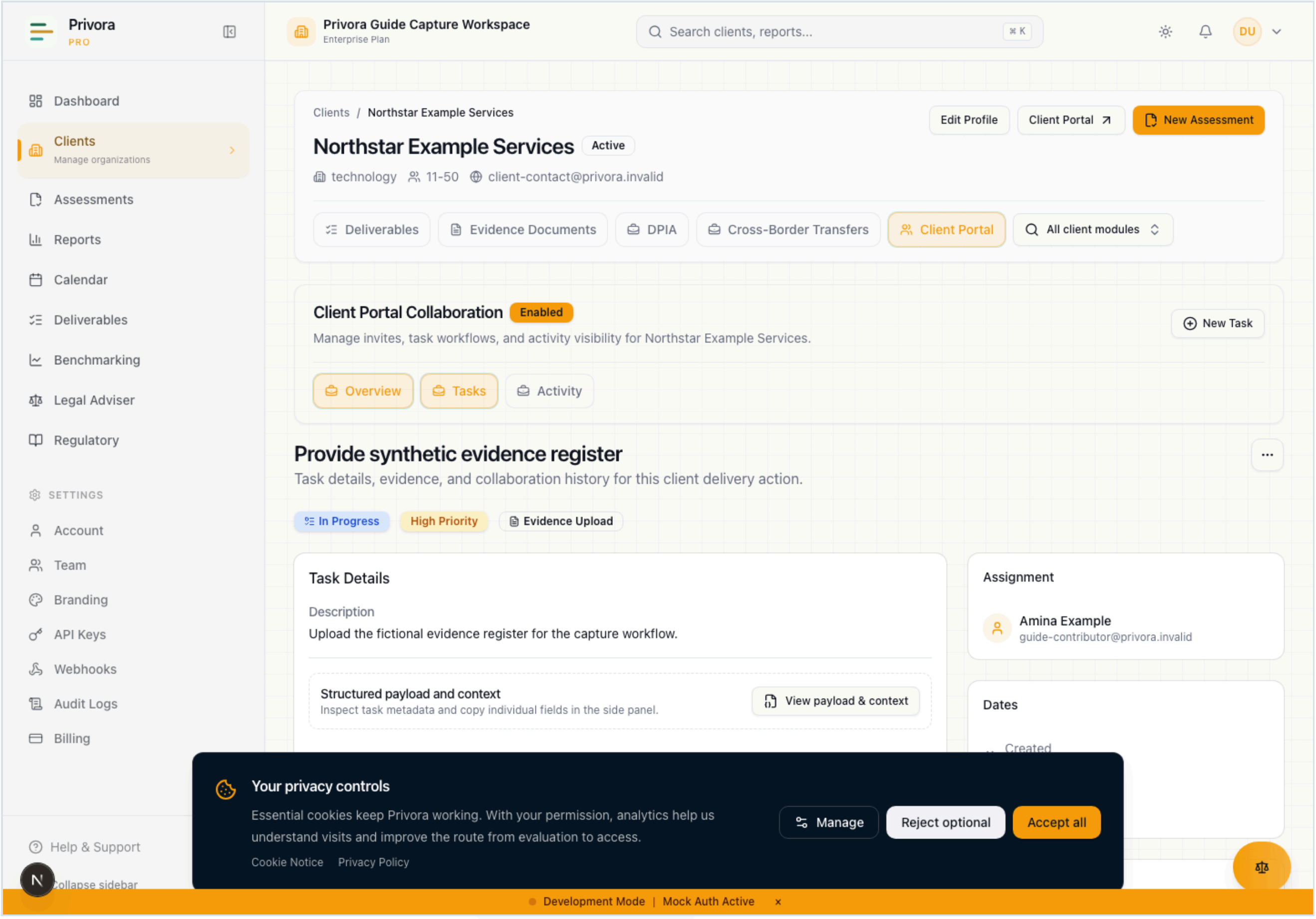


Use the Console evidence tasks view to continue the privacy operations workflow.

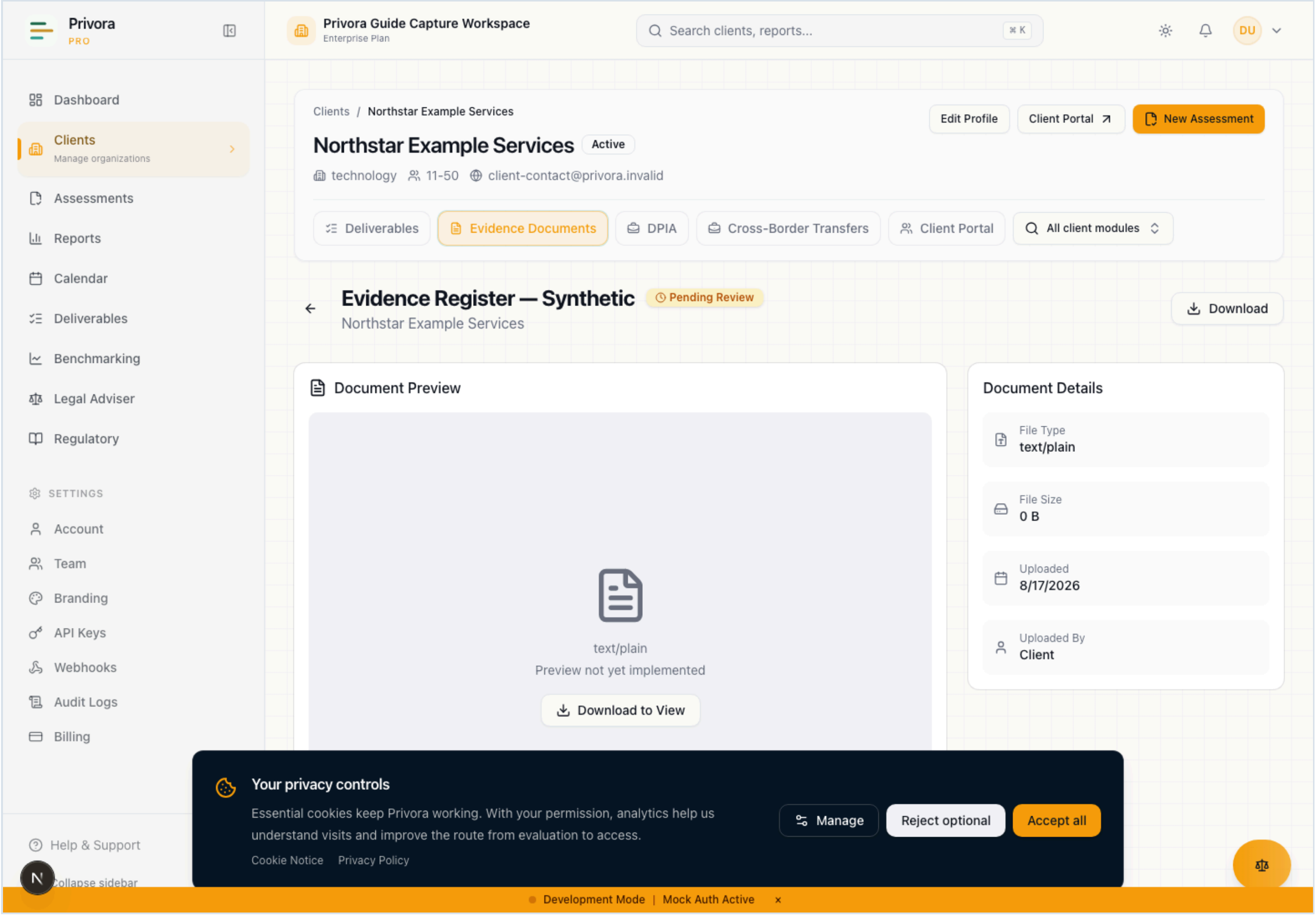
1. Tasks heading

How to reach this page

1. Start on the Console dashboard
2. Open the evidence tasks workflow



Use the Console evidence task detail view to continue the privacy operations workflow.
1. Evidence task heading



Use the Console document review view to continue the privacy operations workflow.

1. Document name

Use this concise path inside authenticated console help to operate the full evidence cycle: Request → Owner → Evidence → Review → Decision → Report. The request owner and evidence reviewer should confirm purpose and authority, progress every stage, resolve returns or exceptions, close the cycle, and update the Privora Pro record. The contributor section later in this runbook explains only assigned portal work and does not replace this operator method.

Outcome and when to use the cycle

Create a traceable chain showing what was requested, who owned the response, what evidence and context were received, who reviewed it against which criteria, what decision was recorded, and where the result informs reporting. Use the cycle for a bounded assessment, requirement, deliverable, remediation check, or management-review need. Do not use it for bulk file migration or as a substitute for a specialist breach, data-subject, privileged, or investigative workflow.

Roles and evidence authority in console

The request owner defines purpose, criteria, due date, and reporting relationship. The evidence owner coordinates an accurate response. A client contributor supplies assigned facts, comments, and files within the client portal but has no approval or exception authority. The evidence reviewer applies accountable human review and records the outcome. The DPO, privacy lead, or engagement lead resolves decisions reserved by the authority model, and the report owner carries reviewed results and limitations into the output. Verify organization and client scope at every lookup and assignment.

Six-stage evidence path

Stage 1 — create a precise console Portal Task with purpose, criteria, safe scope, owner, due date, reviewer, and reporting link. Stage 2 — assign one accountable owner within the same client and confirm the handoff on task detail. Stage 3 — receive the submission with source, period, version, approval context, and limitations; task completion or upload is not approval. Stage 4 — open the client Document, test relevance, authority, currency, completeness, consistency, and proportionality, and apply accountable human review. Stage 5 — record approval for the stated purpose, return or rejection with actionable notes, clarification, or a named exception path. Stage 6 — connect the reviewed result and its limitations to the relevant requirement, workflow, Deliverable, or management report.

Returns, exceptions, and escalation path

Return work when the source, period, version, context, authority, or criterion is insufficient. Preserve the submitted version and request the smallest sufficient correction. Escalate overdue work to the evidence owner and engagement lead; tenant-boundary uncertainty immediately to the authorized access path; and privilege, disputed interpretation, security, sector, suspected falsification, or material conflict to qualified authorities. A named authority must approve an exception with rationale, consequence, interim action, and review date.

Evidence completion and review cadence

Close the cycle only when request, owner, contextual evidence, version, human review, decision rationale, returns or exceptions, reporting link, and next review are traceable. Upload, task completion, or a report draft alone is not completion. Set the review cadence according to evidence volatility and decision risk, and reopen the cycle when the owner, source process, approval, period, or underlying facts materially change.

Privora Pro evidence handoff

Use console Portal Tasks for the request, assignment, dates, status, and collaboration; portal task detail for assigned contribution; Documents and document detail for metadata, linked requirements, versions, and authorized review outcomes; Deliverables for the reporting handoff; and Audit History for available traceability. Enter approved records in those surfaces, keep rationale with the relevant workflow record, link rather than duplicate sensitive material, and verify client, request, owner, version, decision, report, and next-review date before closure.

The operating outcome

The outcome is not a folder containing files. It is a traceable evidence cycle in which the team can answer six questions: what was requested, who owned the response, what evidence and context were received, who reviewed it against which criteria, what decision was recorded, and where the result informs reporting or further work.

The common workflow problem is fragmentation. A consultant sends a broad request by email. A client forwards several files without periods or approval context. A reviewer comments in another channel. A spreadsheet shows “received,” but nobody can tell which version was reviewed, whether the item was returned, or how it affected the deliverable. Reporting then depends on manual reconstruction.

The operational improvement is a controlled sequence with explicit gates. Each request carries purpose and acceptance criteria. One accountable owner coordinates the response. The submission includes context. A named reviewer applies accountable human review. The decision is recorded separately from upload or task completion. The result is connected to the relevant requirement, deliverable, or next action.

This is better because status reflects meaning rather than motion. “Uploaded” means a file arrived. “Task completed” means the contributor completed the assigned portal action. “Approved” or “rejected” reflects a review outcome recorded by the authorized reviewer. Keeping these states distinct reduces repeated evidence chasing, prevents premature reporting, and makes unresolved work visible.

When to use this runbook

Use the runbook when a privacy team needs evidence for an assessment, requirement, client deliverable, management review, remediation check, or another implemented workflow. Use it for a single material item or a bounded request set that can share an owner and review purpose.

Do not use the cycle as a bulk document migration method. A request should exist because a decision, requirement, control, or report needs support. If the purpose cannot be stated, pause before asking the client to upload material. Unnecessary collection increases review burden and privacy risk.

Do not use this general cycle to replace specialist handling for live breaches, data-subject requests, privileged advice, employee investigations, or other sensitive processes. Open or use the relevant workflow and apply its authority, deadline, and data-minimization controls. The evidence cycle can support that workflow only when the relationship is clear and safe.

Begin only after confirming the correct Privora organization, client, request owner, reviewer, and intended output. For a new client, complete enough onboarding to establish tenant boundaries and access. For an established client, verify that roles and portal users remain current.

Use one review cycle per clear decision context. If several files support one criterion, group them under that criterion. If one file is being assessed for unrelated purposes, record the distinct review contexts instead of assuming one approval answers every question.

Roles and authority

The request owner is accountable for the request's purpose, scope, due date, and relationship to the operating workflow. The owner ensures that the contributor understands what is needed and coordinates escalation. Ownership does not mean the owner must create the evidence personally.

The evidence owner is accountable for the underlying business process or record. This person can explain source, period, approval context, limitations, and known changes. The evidence owner may delegate collection, but remains accountable for an accurate response.

The client contributor uses the portal to view assigned work, ask for clarification through the available collaboration path, complete the task, and upload linked evidence where permitted. A contributor provides facts and records. Portal access does not grant authority to approve evidence, alter the privacy team's conclusion, or view other client contexts.

The evidence reviewer tests the submission against the stated acceptance criteria. The reviewer checks relevance, authority, period, completeness, consistency, currency, and limitations. The reviewer records an outcome and rationale. Where the subject requires legal, security, records, technical, or sector expertise, the reviewer escalates rather than guessing.

The DPO, privacy lead, or engagement lead owns decisions reserved by the engagement's authority model. A client sponsor may accept a business commitment or receive a report, but should not be assumed to approve a specialist conclusion. A report owner decides how the reviewed result appears in a deliverable without changing the underlying evidence decision.

Privora organization and client boundaries apply to every role. Console users require current organizational authority. Portal users are scoped to their client and permissions. The server-enforced boundary is authoritative; a visible link or copied identifier is not permission. If client context is uncertain, stop and verify it.

Role	Main responsibility	Must not be assumed
Request owner	Defines purpose, criteria, owner, and due date	That a broad request will become clear after upload
Evidence owner	Coordinates an accurate, contextual response	That delegation removes accountability
Client contributor	Provides assigned facts, comments, and files	That completion or upload grants approval
Evidence reviewer	Applies criteria and records the review outcome	That system status replaces human judgment
DPO or privacy lead	Resolves reserved privacy decisions and escalation	That every item requires the same authority path
Report owner	Links reviewed results to reporting	That a draft report changes evidence status

Define evidence acceptance criteria

Define acceptance before creating the request. State what the evidence should demonstrate, the relevant organization or process, the period covered, acceptable source or authority, minimum context, expected format where necessary, currency threshold, and who will review it. Criteria should be proportionate to the decision.

A useful criterion is observable. “Provide the current approved retention schedule covering customer and employee records, including owner and approval date” is reviewable. “Send all data protection documents” is not. Broad requests create unnecessary collection, unclear completion, and avoidable returns.

Separate required properties from preferences. If a particular format is needed for accessibility or review, explain why. Do not reject reliable evidence solely because it looks different from an internal template. Conversely, do not approve a polished file that lacks authority, relevance, or current context.

Define the outcome vocabulary before review. This runbook uses approved, rejected or returned, clarification required, exception accepted by named authority, and not applicable with rationale. Match the implemented document states where recording a document review, and use workflow notes or decisions for context that the state alone cannot express.

Identify prohibited or minimized content in the request. Do not ask contributors to place passwords, complete identity files, raw special-category datasets, or live incident payloads in general evidence tasks. Ask for a safe extract, summary, controlled reference, or appropriately redacted record when that is sufficient.

Record the relationship to a requirement or output. The current portal task flow can carry linked evidence context, and the document workflow can associate documents with evidence requirements. The reviewer must still determine whether the relationship is valid.

Stage 1 — Create a precise request

Create the request from the correct client's console portal tasks area. Give it an action-led title, concise description, category, priority, due date, and assignee when known. For evidence work, use the evidence category and link the relevant requirement when the implemented option applies.

Create an evidence request · Privora Pro console

Write the brief so a contributor can act without seeing internal deliberation. Include purpose, scope, period, expected evidence, context fields, completion instruction, and clarification path. Exclude cross-client information, internal risk conclusions, unnecessary personal data, and authority the contributor does not hold.

Use one request for one coherent outcome. Split unrelated evidence needs when they have different owners, due dates, criteria, or reviewers. This improves assignment and makes returned work specific. If several closely related files support one criterion, explain how they should be grouped.

Choose a realistic due date that leaves time for review and returned work before the reporting deadline. A contributor due date is not the same as a reviewer decision date. Record both in the operating plan and use Calendar where the broader deadline requires management.

Before sending, perform a request-quality check: correct client, legitimate purpose, minimum necessary scope, named owner, clear criteria, safe submission method, due date, reviewer, and reporting link. The output of Stage 1 is a request that can be understood and audited without a separate email explanation.

Stage 2 — Assign the accountable owner

Assign the portal task to an active portal user for the same client when that person is responsible for coordinating the response. The current task workflow validates client membership for an assignee. Do not use an unassigned task when accountability is material merely because several people could respond.

Open the console task detail to confirm assignment, due date, category, priority, linked context, and collaboration history. The task detail is also the place from which the delivery team can monitor progress and clarify the brief.

Review the evidence task · Privora Pro console

Tell the owner what coordination means: identify the source, preserve the relevant period and version, obtain any internal approval needed before submission, provide limitations, and respond to clarification. The owner should not certify matters outside their authority.

Where the evidence spans functions, keep one accountable owner and name supporting contributors in the collaboration plan. Avoid assigning the same request independently to several people without defining who consolidates the response. Duplicate submissions increase version uncertainty.

If the intended owner cannot access the portal, resolve the access issue through the authorized client portal process. Do not share another person's session, invitation, or task link as a workaround. If the owner changes, update the assignment and communicate the handoff.

Stage 2 ends when the request has one accountable owner, an appropriate contributor path, an identified reviewer, and a known escalation route for delay or uncertainty.

Stage 3 — Receive evidence with context

The contributor should open the assigned portal task, read the brief, confirm the relevant period and source, and use comments or the agreed path to request clarification before submitting unclear material. Where a file is required, the portal task can open the document upload flow with task and requirement context.

Uploading a file is not approval. Completing a task does not constitute an evidence decision. Both actions indicate that the contributor has supplied or completed the requested work and allow the authorized team to begin review.

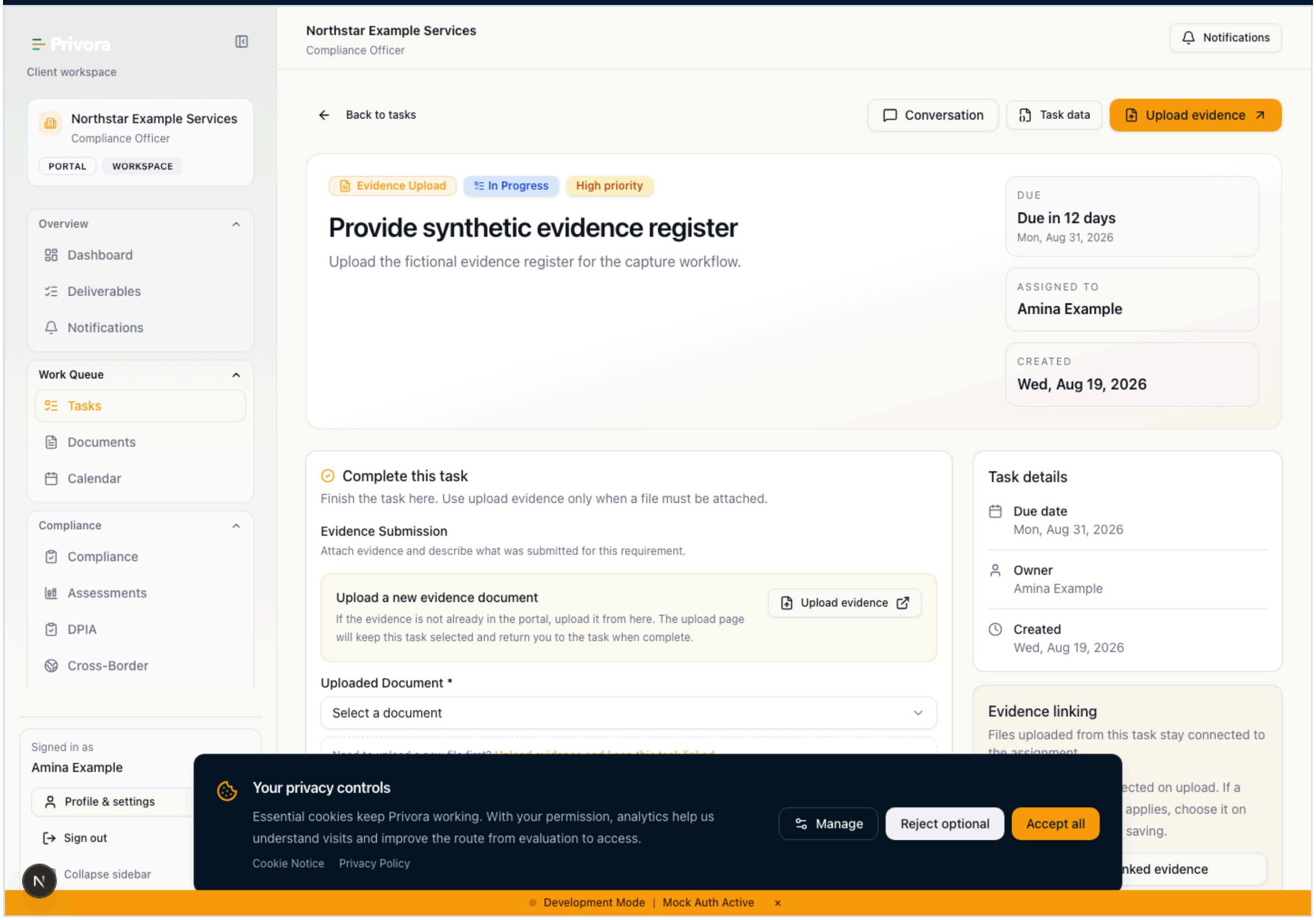
Complete an assigned evidence request

Open only the task assigned within your client portal. Read the request purpose, requested period, due date, and evidence criteria. If the request is unclear or appears to seek information outside your responsibility, ask the engagement owner for clarification through the task collaboration path before submitting.

Provide a safe description of what the evidence demonstrates, its business owner, period, source, approval context, and any limitation. Use Upload evidence only when a file must be attached. Do not include passwords, complete identity records, raw sensitive datasets, or information belonging to another client.

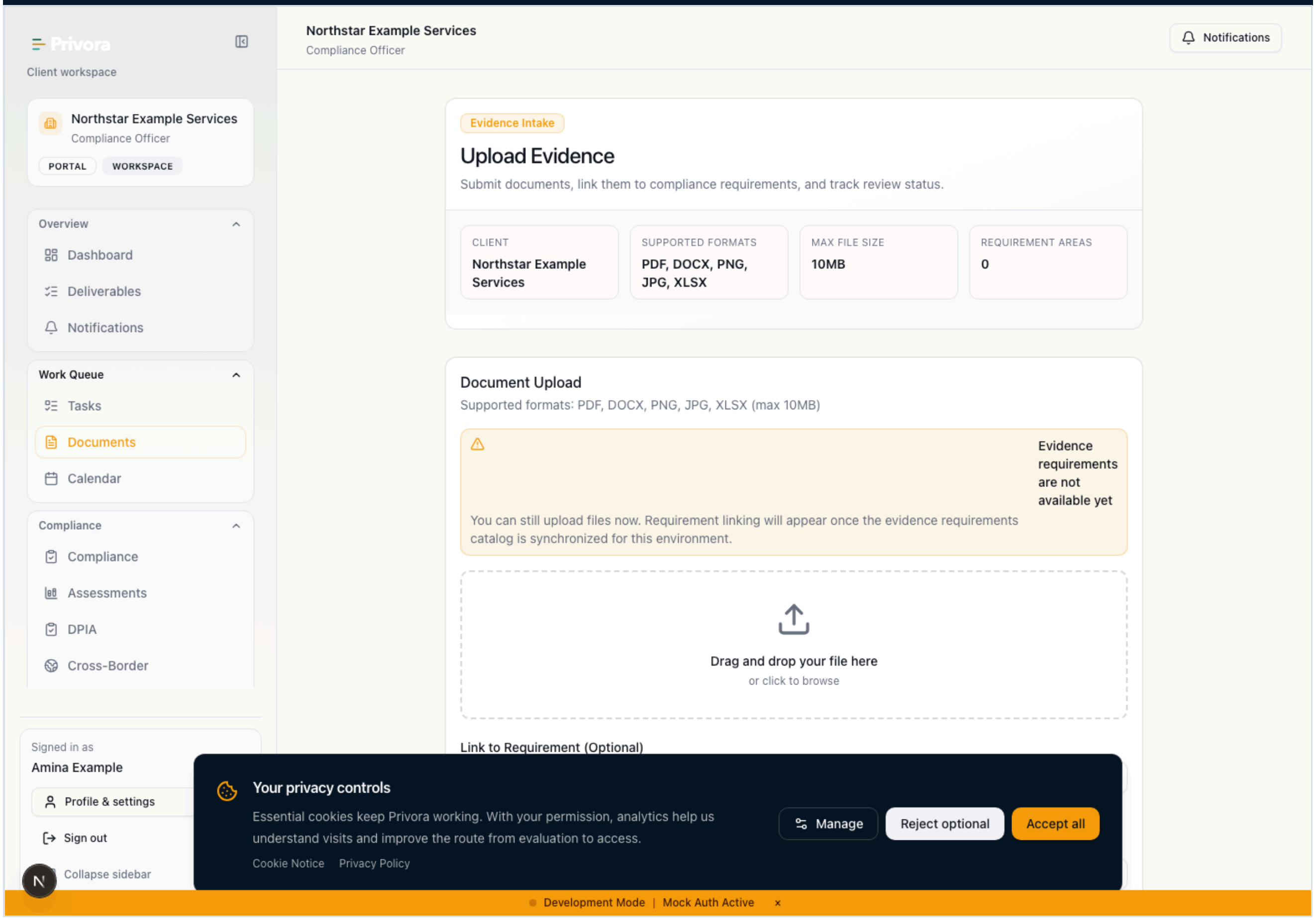
Complete the task after the requested response and required file are supplied. Completion records your contribution; it does not approve the evidence. After review, check the task, document status, notification, or engagement-owner feedback for the post-review status. Respond to a returned item with the requested clarification or a new version rather than replacing context silently.

Open the assigned evidence task · Privora Pro client portal



Use the Portal evidence task view to continue the privacy operations workflow.

1. Evidence task heading



Use the Portal document upload view to continue the privacy operations workflow.
1. Upload heading

Preserve submission context in the authorized record. Include a meaningful file name, category, period, description, owner, and relationship to the request or requirement. The current document workflow retains version information; use a new version when addressing returned work rather than disguising a change as the original item.

Use the portal document upload route only within the contributor's permission and client context. The uploader should not infer that seeing an option grants authority beyond the assigned client. If a record cannot be safely uploaded, use an approved controlled reference and escalate the access method.

Open portal evidence upload

Stage 3 ends when the submission and its context can be connected to the request, owner, period, and version. A file without sufficient context remains incomplete even if the task is marked completed.

Stage 4 — Review sufficiency and currency

Review from the correct client Documents area. Pending documents are awaiting review. Open the document detail to inspect available metadata, linked requirements, version, uploader context, and review controls. Apply the criteria defined before the request.

Review client evidence documents · Privora Pro console

Open the evidence document · Privora Pro console

Test relevance: does the item address the stated criterion and correct client scope? Test authority: is the source and approval context credible for the purpose? Test period and currency: does it cover the required time and remain current enough for the decision? Test completeness: are material sections, attachments, or explanations missing? Test consistency: does it conflict with another approved source or known workflow state?

Apply accountable human review. Automated summaries, file names, task completion, linked requirements, or prior approvals can inform the review, but they do not make the current decision. The named reviewer remains answerable for the recorded outcome and escalation.

Use proportionality. A low-risk operational confirmation may need less formal support than a material regulatory or management assertion. Document why the level of evidence is appropriate. Do not increase collection merely to make the file set look substantial.

If evidence is insufficient, write review notes that are specific and actionable: what criterion was not met, what context or revision is required, who should respond, and when the decision will be revisited. Avoid vague rejection language. If evidence conflicts with another source, preserve both references and escalate the conflict.

Stage 4 ends when an authorized reviewer has enough information to record a decision or has clearly returned the work for defined clarification.

Stage 5 — Record the decision

Record the document review outcome using the implemented review control where appropriate. Current document review supports approved or rejected outcomes for pending documents and retains reviewer context, review time, and optional notes. Use notes to explain the criterion and limitation; do not rely on status alone for a material decision.

Approval means the evidence is accepted for the stated purpose and review context. It is not a universal statement about the entire organization, control, or compliance posture. If the same item will support another decision, check whether the original review criteria and period remain applicable.

Rejection or return means the current item does not satisfy the stated criteria. Preserve the submitted version and rationale. Ask for a new version or clarification through the appropriate task or collaboration path. Do not delete inconvenient evidence merely to simplify the record.

Where an exception is accepted, name the authority, rationale, consequence, compensating action, and review date. A contributor cannot accept the exception through task completion. A reviewer should not accept an exception outside their mandate.

Separate evidence decision from workflow decision. Approved evidence may still reveal a control gap. Rejected evidence may reflect poor context rather than a failed control. Record the next operational action so reports do not collapse these different meanings into one label.

Stage 5 ends with a dated outcome, reviewer, rationale, scope, next action, and escalation where required. If the reviewer cannot make the decision, the recorded outcome is “requires named review,” not an assumed approval.

Stage 6 — Connect the result to reporting

Connect reviewed evidence to the requirement, assessment, deliverable, or management report it supports. Use links and references available in the product rather than copying the full document or review rationale into every downstream record. Preserve the evidence status and limitation when summarizing it.

Use Deliverables to track the client-facing output where applicable. A generated or drafted deliverable remains a draft until the named reviewer or approver accepts it. The report owner should verify that every material statement is based on reviewed evidence, clearly identified assumptions, or visible gaps.

Review client deliverables · Privora Pro console

Report the difference between evidence health and outcome. A complete evidence set can support a finding that work remains. A missing evidence item can create uncertainty without proving that the underlying control is absent. Use careful language: reviewed, pending, returned, exception, not applicable with rationale, or unresolved.

Record follow-up actions with owners and dates. If the decision changes a priority, deadline, assessment response, or deliverable, update the relevant operating record. Avoid maintaining an independent evidence-status spreadsheet that can drift from Privora Pro.

Stage 6 ends when the reviewed result is connected to the intended output, limitations remain visible, and unresolved work has a named owner and review point.

Returned work, exceptions, and escalation

Return work when criteria are unmet, context is missing, a version is unclear, the period is wrong, authority is absent, or the item conflicts with another source. State the smallest sufficient correction. Use a new version where the document changed and preserve the original history.

Escalate overdue work to the evidence owner and engagement lead before it silently blocks reporting. Explain the consequence and revised decision date. If the due date derives from a regulated workflow, follow that workflow's verified escalation rules rather than inventing an extension.

Escalate cross-client or tenant-boundary uncertainty immediately. Do not open, transfer, link, or summarize evidence until the correct client context is confirmed. Record a safe incident or support reference without duplicating exposed information.

Escalate privilege, disputed legal interpretation, material security concerns, sector-specific requirements, suspected falsification, or serious conflicts to qualified authorities. Do not ask a portal contributor to resolve an internal risk or approval decision.

Accept an exception only through the named authority model. Record why normal criteria could not be met, the residual uncertainty, interim control, expiry or review date, and effect on reporting. An undocumented exception becomes invisible risk.

Completion and review cadence

The cycle is complete when the request and purpose are preserved; an accountable owner is named; the received evidence has source, period, version, and limitation context; a named reviewer applied the criteria; the decision and rationale are recorded; returned work or exceptions are resolved or owned; and the result is linked to the intended report or workflow.

Task completion alone is not cycle completion. Upload alone is not cycle completion. A report draft alone is not cycle completion. The six-stage chain must remain traceable from request to report.

Set a review cadence based on evidence volatility and decision risk. Review high-change operational evidence more often than stable approved material. Record expiry dates or next-review dates where relevant. Reopen the cycle when ownership, source process, approval, period, or underlying facts materially change.

At cycle close, ask whether the request was clear, the owner was appropriate, the contributor supplied enough context, review criteria were proportionate, the decision was understandable, and reporting preserved limitations. Use the answers to improve the next request rather than adding unnecessary fields.

Record the work in Privora Pro

Use console Portal Tasks for the request, accountable assignment, due date, status, and collaboration. Use portal task detail for the contributor's assigned action and linked upload path. Use Documents and document detail for evidence metadata, requirement links, version context, and authorized review outcome. Use Deliverables for the client-facing reporting handoff and Audit History for traceability available to authorized roles.

Review Audit History when you need to verify relevant document, client, report, or team activity. An audit event supports traceability but does not contain every decision reason. Keep the rationale with the relevant task, document review, exception, or deliverable record.

Review audit history

Keep approved information in the authorized Privora Pro workspace. Use the workbook to prepare the request and review, then enter approved records in the appropriate product surfaces. Do not maintain a second final status in email or the workbook.

Before closing, verify the correct organization, correct client, request ID, owner, task status, document version, review outcome, reporting link, and next-review date. This control makes the operating record explainable to someone who did not participate in the original exchange.

Sources and professional review

Product behavior and routes were reviewed against the current Privora Pro workflow source of truth and implemented task, portal, document, deliverable, and audit pages on 2026-08-12. The brand and product-marketing sources define Privacy Operations as the category and set the evidence, ownership, review-readiness, and claim boundaries used here. This runbook does not assert a statutory evidence-retention period or universal review frequency.

Implemented portal-task, document-review, deliverable, audit, and client-scope behavior; reviewed 2026-08-12

Privacy Operations category, evidence and ownership language, and claim boundaries; reviewed 2026-08-12

Audience needs, evidence pain points, operational differentiation, and customer language; reviewed 2026-08-12

Apply current internal policy, client agreements, verified regulatory sources, and qualified professional judgment to the particular evidence purpose. If product behavior, documentation, client facts, or authoritative material conflict, stop the affected instruction, preserve the conflict, and obtain the appropriate decision before presenting the evidence as approved.