Privora

PRIVACY OPERATIONS · PRIVORA PRO · RUNBOOK

Handle a data subject request as a controlled workflow

Run one owned request record with proportionate identity verification, scoped searches, visible decisions, reviewed delivery, and retained history.

Primary action

Start the request record 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.

Handle a data subject request as a controlled workflow

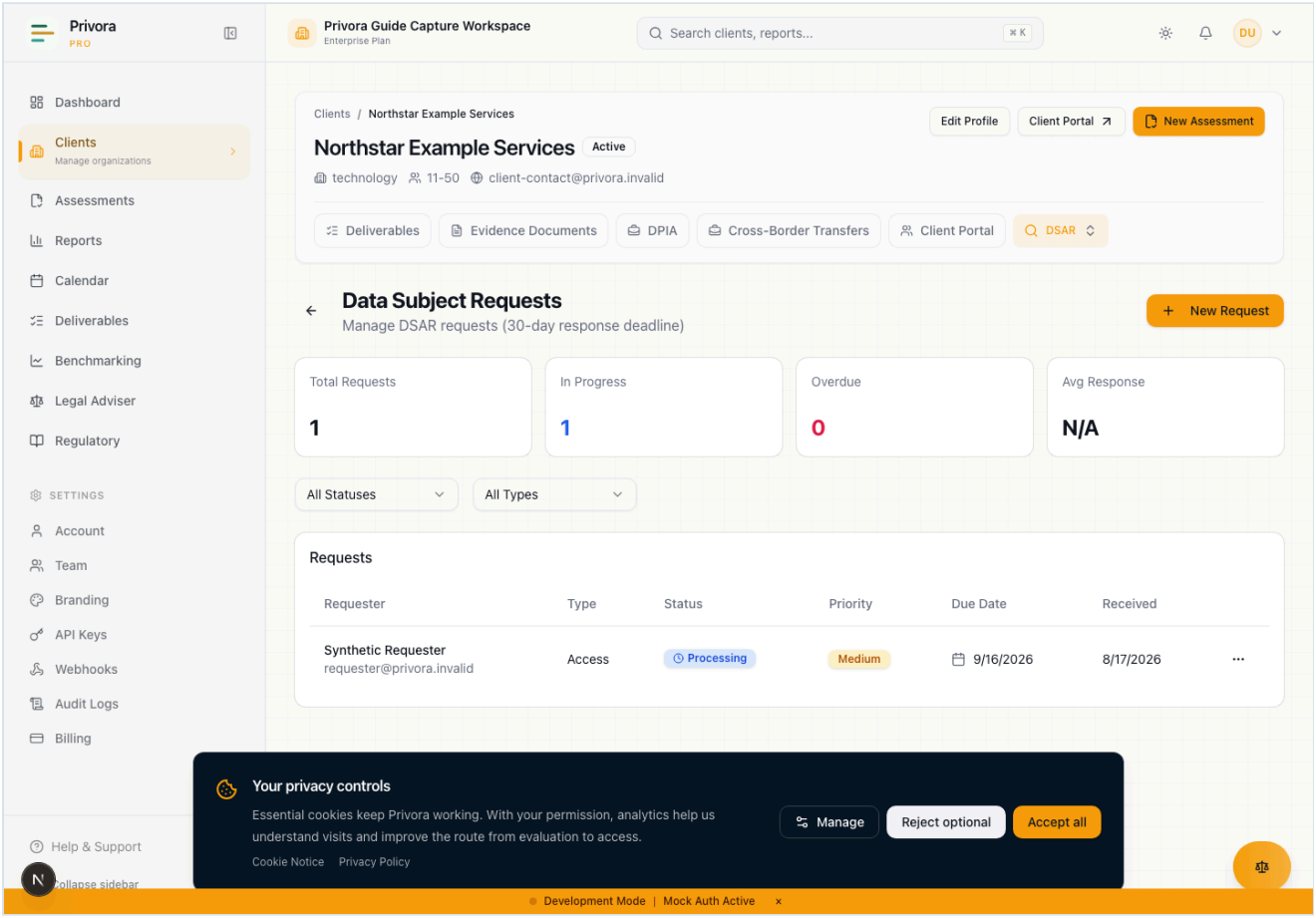
> Operational guidance — not legal advice. This guide does not guarantee compliance.

Apply this method with qualified privacy, legal, records, security, and sector review. Completed request material is confidential. Keep identity evidence, response data, restrictions, delivery evidence, and communications in approved systems. Privora Pro remains the operating record after reviewed information is entered.

The operating outcome

Product walkthrough

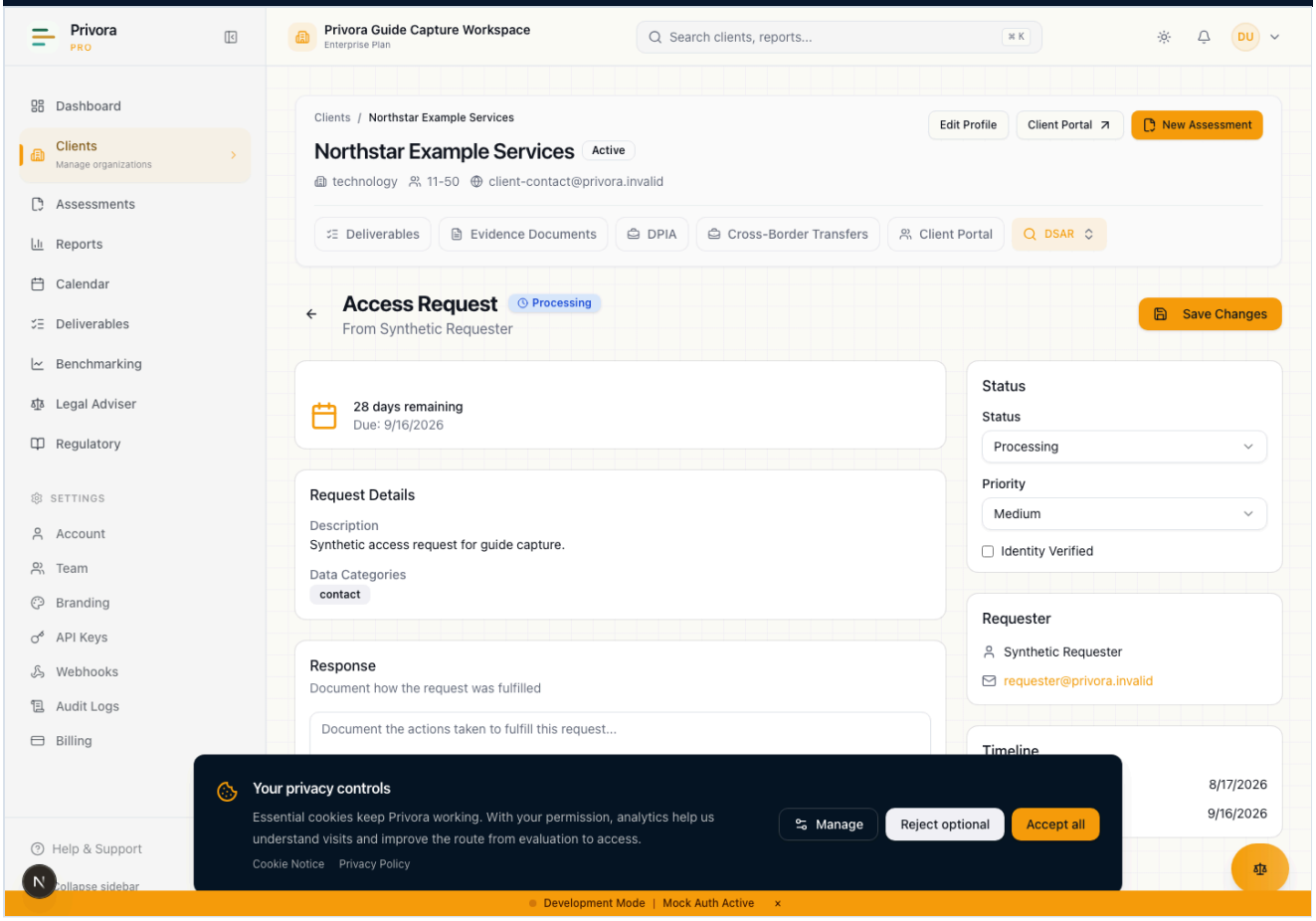
Open the client workspace, choose DSAR, and use the request detail page to confirm intake, ownership, search work, review, and delivery status. Use the portal task only for an assigned contribution; approval and final response remain in the controlled console workflow.



Use the Console dsar list view to continue the privacy operations workflow.
1. DSAR heading

How to reach this page

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



Use the Console dsar detail view to continue the privacy operations workflow.
1. DSAR request heading

A well-run data subject request is a controlled chain of decisions. The organisation can show when the request arrived, how it understood the request, why the identity check was proportionate, where owners searched, what was found, which information required protection or qualified review, who approved the response, how it was delivered, and why the record was closed.

This runbook is for DPOs, DPCO teams, request owners, records owners, system owners, legal reviewers, and client contributors. It improves the workflow from intake to closure. It is better than inbox handling because ownership, status, due date, activities, and reviewed response remain connected. It reduces complexity by separating the requester's rights, contributor searches, privacy-team judgment, response approval, and delivery authority.

Privora Pro records request type, requester details, received and due dates, priority, identity state, assignment, activities, response information, and closure status. Operators remain responsible for accurate facts, legal interpretation, restrictions, communication, and secure delivery. The system's due date is an operational product target; it is not itself proof of the deadline required by Nigerian law or another applicable rule.

When to use this runbook

Use the workflow when a person asks about personal data or exercises a right relating to access, correction, erasure, restriction, objection, withdrawal, automated decision-making, or portability. A request does not need legal language, a form, or the correct department. Train frontline teams to recognise a request and route it promptly without forcing the person to start again.

Also use the method for requests arriving through customer support, HR, a branch, social media, a representative, a regulator referral, or another business channel. Record the original words and channel, then classify the request after review. Separate a privacy-rights request from a complaint, litigation hold, fraud alert, or ordinary account query, while coordinating related processes where necessary.

The official NDPA section 34 gives a data subject rights without constraint or unreasonable delay, including confirmation and access information, a copy in a commonly used electronic format subject to the

Act's cost qualification, correction or deletion of inaccurate information, erasure in stated circumstances, and restriction pending specified resolution. Sections 35–38 address withdrawal, objection, automated decisions, and portability. These rights require fact-specific interpretation; this runbook does not decide their application automatically.

Sections 34–38, official PDF pp. A738–A740

Roles and authority

Role	Accountable work	Authority boundary
DPO or privacy lead	Classify the request, set the reviewed approach, resolve privacy questions, and oversee response quality	Does not assume facts that search owners must verify
Request owner	Coordinates intake, assignments, dates, communications, approval, delivery, and closure	Does not make legal restriction decisions without qualified review
Records or system owner	Searches the assigned scope, preserves context, and returns complete results or a documented nil result	Does not decide the request or communicate the final response
Identity reviewer	Chooses and performs a proportionate check through an approved channel	Does not retain unnecessary identity material
Legal or specialist reviewer	Advises on restrictions, competing rights, privilege, holds, sector rules, and redaction	Advice and decision must be recorded by the authorised owner
Response approver	Confirms completeness, legal review, security, delivery method, and communication	Approval cannot be delegated to a portal contributor
Client portal contributor	Completes a scoped assigned search or fact request	Cannot classify, restrict, approve, deliver, extend, or close the request

Name a request owner at intake and an alternate for absence. Restrict access to the client and request. Do not expose all requests to a contributor merely because they own one system. Contributions should use assigned tasks with clear acceptance criteria and safe evidence references.

Stage 1 — Record intake and acknowledge the request

Owner: request owner. Inputs: original request, channel, received time, requester contact, and any representative information. Output: a traceable request record and controlled acknowledgment.

Preserve the requester's original words. Record when the organisation received it, who received it, the channel, contact details needed to respond, and any immediate accessibility or safety need. Avoid copying unrelated account history. If the request includes sensitive material, place it in the approved restricted location and reference it.

Create the request under the correct client. Choose an initial type without narrowing the person's words. Assign priority based on risk, vulnerability, active harm, legal hold, or operational urgency, not on seniority.

Name the owner and set an internal triage date.

Send an acknowledgment through an approved channel. Confirm receipt, explain what happens next, identify a contact route, and request clarification only where necessary. Do not promise an outcome, quote an unsupported deadline, or ask for identity documents by ordinary email.

Record in Privora Pro: type, requester contact, description, safe category labels, received date, priority, internal assignment, and an activity for the acknowledgment. Privora Pro remains the operating record, while communication evidence stays in the approved system.

Stage 2 — Verify identity proportionately

Owner: identity reviewer with request-owner oversight. Inputs: request channel, existing authenticated relationship, risk of disclosure, representative authority, and available verification methods. Output: recorded method and result without unnecessary identity data.

Use proportionate identity verification. Start with information or an authenticated channel the organisation already uses. Increase assurance where the response could reveal sensitive data, the request changes account control, or fraud indicators exist. Do not demand a government document for every request by default, and do not collect more identity information than is necessary for the risk.

For a representative, verify both the requester's identity as appropriate and the representative's authority. For a child or person lacking capacity, obtain qualified review of the applicable authority and safeguards. If identity cannot be established, explain what is needed and keep the request open or restrict action according to the reviewed procedure rather than silently rejecting it.

Record the method, date, reviewer, result, and evidence reference. Do not copy a full identity image into the notes. Where a document was checked, retain it only if the approved policy requires retention and protect it accordingly.

Decision point: proceed when assurance is proportionate to the response risk; escalate ambiguity or suspected impersonation. Record in Privora Pro: identity status and method using a minimal description.

Stage 3 — Classify and scope the request

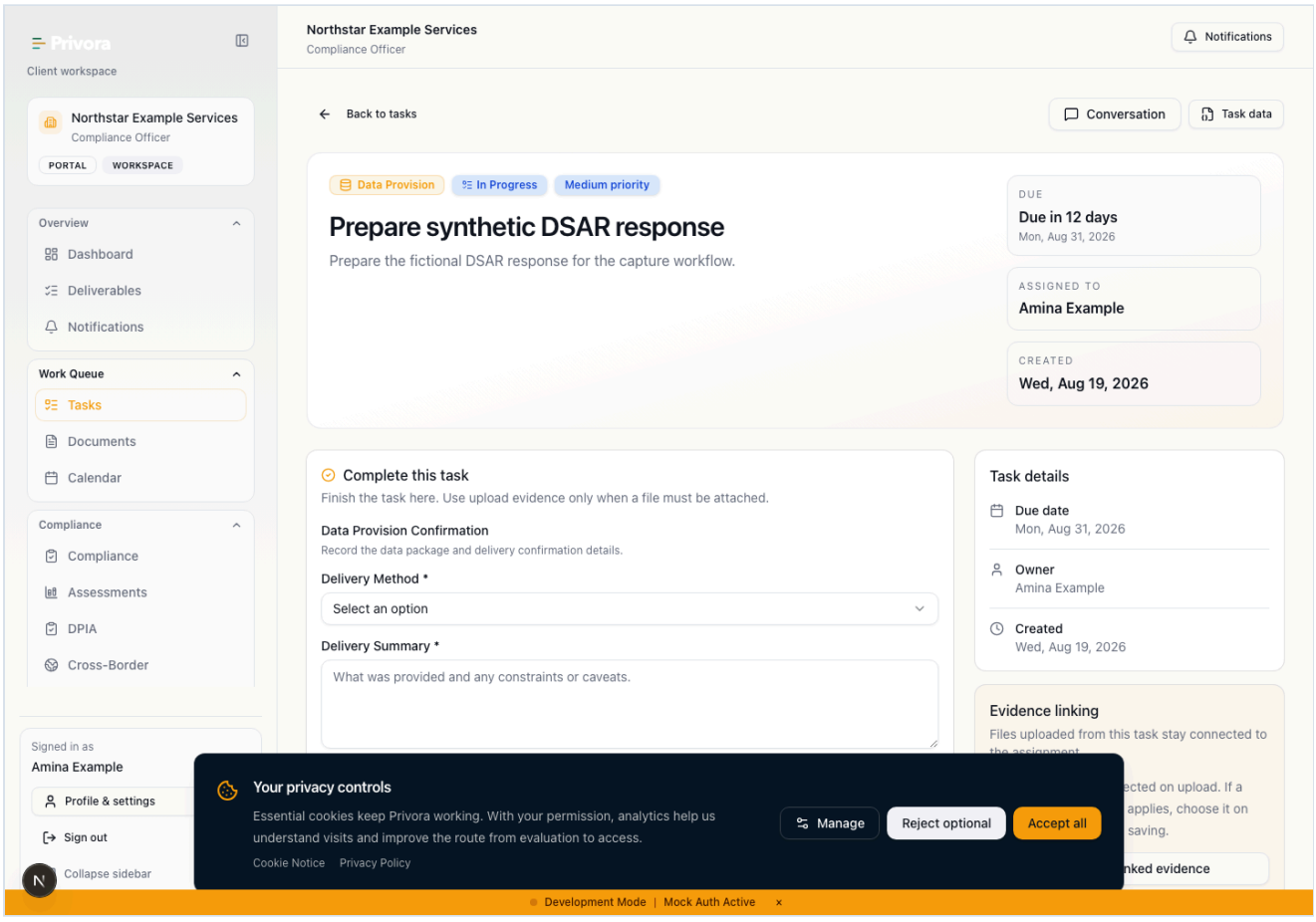
Owner: DPO or privacy lead with the request owner. Inputs: original request, clarification, identity result, data map, processing records, and applicable rights. Output: scope statement, work plan, and reviewed deadline.

Map the person's words to one or more request types without discarding broader meaning. Identify people, accounts, identifiers, date range, business units, products, systems, processors, communication channels, and likely formats. Distinguish personal data about the requester from data about other people, corporate records, and material outside the request.

Clarification can make a broad request workable, but it should not become a barrier. State what the team will search while clarification is pending and retain the communication. Consider whether preservation or processing restriction is needed while the request is resolved.

Set the organisation's reviewed deadline from current official requirements, applicable sector rules, facts, and qualified advice. Record the source and review date. Treat the product due date as an operational target that needs confirmation, not as proof of the legal rule. Name intermediate dates for searches, review, approval, and delivery.

Record in Privora Pro: update the type, description, categories, priority, owner, and reviewed operating plan. Use activities or approved referenced records for the detailed scope and communications.



Use the Portal dsar task view to continue the privacy operations workflow.
1. DSAR task heading

Stage 4 — Assign searches to systems and owners

Owner: request owner. Inputs: agreed scope, system map, identifiers, date range, search method, and acceptance criteria. Output: assigned searches with complete or documented nil results.

Break the scope into assignments. Each task should name the system or record set, safe identifiers, date range, formats, included and excluded areas, expected evidence, due date, and escalation contact. Use a

task for a scoped contribution rather than giving the contributor the full request record where it is not needed.

If you receive an assigned portal task, search only the stated scope. Return the systems checked, query or method at a safe level, period covered, result location, gaps, and any dependency. A nil result needs the same context as a positive result. Do not paste response data, passwords, full identity records, raw sensitive data, or restricted third-party information into comments. Store material in the approved workspace and provide its reference.

Completing a search contribution does not grant approval or decision authority. It also does not grant authority to classify, restrict, redact, deliver, extend, or close the request. The privacy team evaluates the result, may return it for clarification, and decides whether further searches are required.

Open assigned request search task · Privora Pro client portal

Stage 5 — Compile and review the response set

Owner: request owner with records and privacy review. Inputs: search returns, source records, processing information, notices, recipient and retention facts. Output: deduplicated response inventory and review set.

Log every assignment and result. Confirm that expected owners responded, gaps are visible, and late sources are escalated. Deduplicate without losing source, date, context, or version. Separate the data set from explanatory information such as purpose, categories, recipients, retention, source, rights, and automated-decision information where applicable.

Check that identifiers match the requester and that records belong to the correct client. Detect information about other people, privileged or confidential content, security-sensitive detail, active investigations, legal holds, or records whose disclosure may cause harm. Flag these for qualified review rather than deleting them from the inventory.

Use a controlled review location. Give files stable references and track decisions at item or category level. Avoid creating extra uncontrolled copies merely for convenience. Check the requested format and accessibility needs early enough to prepare a usable response.

Record in Privora Pro: update status and response preparation facts at the appropriate level; retain detailed source material in approved document controls and reference it from the request history.

Stage 6 — Resolve restrictions, exemptions, and redactions

Owner: DPO or privacy lead with qualified legal or specialist review. Inputs: flagged response inventory, competing rights, applicable law, sector requirements, holds, and security analysis. Output: reasoned decision log and reviewed redactions.

Do not use a blanket exemption label. For each restriction, identify the item or category, the right engaged, the competing interest or rule, the decision-maker, source, rationale, and effect on the response. Consider whether partial disclosure, separation, pseudonymisation, summary, or another safeguard can protect others while respecting the request.

Redaction must be reviewable. Record why information was removed and perform a second-person quality check. Ensure hidden content, comments, metadata, layers, formulas, revision history, filenames, and attachments do not reveal restricted information. Preserve the unredacted source under appropriate access controls.

Where the request relates to objection or automated decision-making, confirm human intervention, the person's opportunity to express a view, and contest routes where applicable. For portability, confirm the current legal basis, technical feasibility, format, recipient validation, and any regulations or conditions that qualified reviewers identify.

Decision point: unresolved legal interpretation, conflict, or high-risk disclosure goes to the named specialist and response approver. Record in Privora Pro: retain the outcome and safe rationale; do not place privileged advice in a broadly visible field.

Stage 7 — Approve and deliver the response

Owner: response approver and request owner. Inputs: response set, decision log, redaction quality check, communication draft, delivery plan, and deadline review. Output: authorised response delivered through a controlled channel.

The approver confirms scope, identity assurance, search completeness, restrictions, format, accessibility, security, recipient, communication, and timing. Compare the response with the original request and later clarification. Confirm that an adverse or partial outcome is explained as required by the reviewed process and includes appropriate complaint or contact information.

Choose delivery assurance based on sensitivity and recipient risk. Validate the address or account independently where appropriate. Do not send passwords with the protected file in the same channel. Confirm access expiry and retry support when using a secure link. Keep evidence of delivery without duplicating the response contents in activity notes.

If delivery fails, preserve the error, investigate the address or channel, and contact the requester safely. Do not mark the request complete merely because a message was sent.

Record in Privora Pro: record approval, response details at a safe level, status, delivery date and method reference, and the accountable approver. Product status is an operational record, not proof that every applicable requirement has been met.

Stage 8 — Close the record and preserve history

Owner: request owner. Inputs: approved response, delivery evidence, open questions, commitments, and retention rules. Output: closed request with reviewable history and lessons.

Confirm delivery or the reviewed reason for another outcome. Resolve returned communications, follow-up questions, and promised actions. Check that search tasks, decision records, approvals, and exceptions are linked and that unnecessary working copies are removed under approved policy.

Record the completion date and final status. A rejected status needs a reviewed basis and communication; it is not a shortcut for difficult searches. Retain the minimum request history needed for accountability, dispute handling, and reporting. Apply access and retention rules to the request record itself.

Review what caused delay, duplicate work, search gaps, identity friction, or unsafe copying. Assign improvements to the data map, notices, retention, system search capability, owner training, or delivery controls. Feed systemic issues into the relevant Privacy Operations workflow.

Record in Privora Pro: complete or reject only after authority and communication checks, retain activities, and record the improvement owner. Privora Pro remains the operating record after closure.

Deadline and extension control

The official NDPA text reviewed for this guide does not establish one universal numeric response period for every request in sections 34–38. Section 34 uses without constraint or unreasonable delay, and sections 34 and 38 also use without undue delay for specified actions. Do not convert the current Privora Pro due-date behavior into a statement of Nigerian law.

At intake, establish the organisation's reviewed deadline using current official sources, request type, sector rules, contracts where relevant, litigation or regulator directions, and qualified advice. Record the source, reviewed date, accountable owner, and intermediate milestones. If several rules apply, use the controlling reviewed position and document why.

Do not promise an extension merely because work is difficult. Only use an extension where a current authoritative rule and the facts support it, after qualified review. Record the basis, decision-maker, revised internal plan, requester communication, and remaining safeguards. If no extension is supported, escalate resources and scope questions without silently moving the due date.

Monitor elapsed time, search completion, review, approval, and delivery. The product calendar supports operational control, but the request owner must reconcile its target with the organisation's reviewed deadline. Escalate immediately when delay is likely.

Section 34(1)–(2) and section 38(2), official PDF pp. A738–A740

Exceptions and escalation

Escalate identity disputes, representative authority, requests involving children or vulnerable people, active harm, suspected impersonation, cross-client records, missing systems, processor delay, legal holds, competing rights, privileged material, security-sensitive disclosure, portability feasibility, failed delivery, or likely delay.

Record the issue, owner, decision needed, interim safeguard, source, and date. Do not hide uncertainty by marking a search complete. Keep the requester informed where the reviewed process requires it, using plain language and an accessible channel.

If a contributor can see information outside the assigned task, stop and correct access before continuing. If requested data could expose another person or a secret, move it to restricted review. If the request reveals inaccurate data, weak retention, or an unsafe automated decision, route the underlying corrective work to an accountable owner rather than treating the response as the end of the issue.

Completion criteria

The current request is complete only when:

- original intake, received time, channel, requester contact, and acknowledgment are traceable;
- identity assurance is proportionate, minimal, and recorded without unnecessary identity copies;
- classification and scope preserve the requester's meaning;
- the organisation's reviewed deadline and source are recorded and monitored;
- every system and records assignment has a contextual result or visible gap;
- response data is deduplicated, source-aware, and reviewed for other people and sensitive context;
- restrictions, redactions, objection, automated-decision, or portability questions have qualified decisions where required;
- approval and secure delivery are evidenced without duplicating response content;
- status and completion date match the actual outcome;
- history, exceptions, communications, and improvement owners are retained; and
- contributor activity stayed within scoped task authority.

Completion demonstrates a controlled operational process. It does not guarantee a legal outcome and does not prevent the requester from asking follow-up questions or using available complaint routes.

Sources and professional review

Regulatory statements were reviewed on 12 August 2026 against the official local Nigeria Data Protection Act 2023 PDF, sections 34–38. Those provisions cover access and related information, correction, erasure and restriction, withdrawal of consent, objection, automated decision-making safeguards, and portability. They do not prove a universal numeric deadline or extension for every request.

Sections 34–38, official PDF pp. A738–A740

Implemented DSAR register, detail, activity, identity, due-date, portal-task, and calendar behavior; reviewed 2026-08-12

Product instructions were checked against current Privora Pro routes and services. Regulatory extracts in Pro documentation were used only to navigate to the official PDF. Confirm current official guidance, sector rules, organisational authority, and delivery safeguards for the facts of each request.