Privora

PRIVACY OPERATIONS · PRIVORA PRO · WORKBOOK

Prepare and control a DPIA decision record

Prepare each decision input on a controlled working page before reviewed information is entered into the staged Privora Pro workflow.

Primary action

Prepare the assessment, then record reviewed information 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.

Prepare and control a DPIA decision record

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

This blank workbook supports preparation. It is not the approval record and does not submit anything to the NDPC. Treat completed pages as confidential working material. Privora Pro remains the operating record after reviewed information is entered.

Data-minimisation rule: Do not record passwords, secrets, raw sensitive data, full identity documents, live credentials, exploitable security detail, or unnecessary personal data here. Store source evidence in the authorised Privora Pro workspace and use references on these pages.

How to use the working pages

Complete the pages with the responsible owners, mark assumptions, and identify the source for each material fact. The privacy lead reviews contributions before transferring approved information into Privora Pro. A contributor may prepare a response but cannot change formal risk ratings, record a regulator outcome, certify the DPO review, or approve processing.

Use concise references rather than copying evidence. If a field needs sensitive operational detail, record a safe evidence ID and location. Date decisions and retain the current workbook version with the engagement's approved records policy.

Page 1 — Workflow charter

Define the decision this DPIA must inform and the operating boundary around it.

DPIA title

Authorised Privora Pro client workspace

Processing stage

☐ Planned
☐ Pilot
☐ Ongoing

Date the assessment must inform the processing decision

Decision this assessment must support

Page 2 — Roles and authority

Name individuals, not only departments. Confirm who may contribute, evaluate, recommend, approve, and communicate externally.

Privacy lead or DPCO consultant

Business or system owner

Security or control owner

Authorised management reviewer

Certified DPO reviewer

Segregation, conflict, or authority exceptions requiring escalation

Page 3 — Trigger and timing screen

Record why the activity may create high risk and what must remain paused until the assessment informs the decision.

Potential high-risk triggers

- ☐ Profiling or scoring
- ☐ Automated decision with significant effect
- ☐ Systematic monitoring
- ☐ Sensitive data
- ☐ Vulnerable people
- ☐ Innovative technology
- ☐ Large scale
- ☐ Public surveillance
- ☐ Cross-border transfer
- ☐ Other reviewed trigger

Connection between the selected trigger and possible rights impact

Processing, procurement, pilot, or launch activity held behind the assessment gate

Source or evidence reference for the trigger decision

Page 4 — Scope and data flow

Prepare a reviewer-readable description from collection through deletion. Use a separate approved diagram where necessary and reference it here.

Nature, scope, context, and purpose of processing

Affected groups, vulnerability factors, and approximate scale

Personal and sensitive data categories using safe category names only

Approved data-flow or architecture evidence reference

Retention, deletion, processing locations, and hosting locations

Recipients, processors, purposes, locations, and contract status

Controls that detect purpose or scope expansion

Page 5 — Lawful basis, necessity, and alternatives

Prepare the analysis for qualified review. A selected label does not establish a lawful conclusion.

Claimed lawful basis and purpose-specific rationale

Why the purpose cannot reasonably be achieved with less personal data

Benefits, intrusion, affected interests, and proportionality analysis

Less intrusive alternatives and disposition

Page 6 — Contribution register

Plan scoped requests. Do not paste portal responses here; reference the task and record the privacy team's review result.

Contribution	Contributor role	Acceptance criteria	Privora task reference	Review owner
Processing context	Business owner	Complete flow, systems, recipients, retention		
Control evidence	Security owner	Period, control, operation, gap, evidence reference		
Stakeholder view	Relevant representative	Rights, fairness, CIA impact, recommended change		
Management recommendation	Authorised reviewer	Go ahead, modify, or stop recommendation with conditions		

Missing, conflicting, returned, or late contributions

Privacy-team evaluation of contribution quality and effect

Page 7 — Vulnerability and rights impact

Assess impact from the data subject's perspective, not only the organisation's security perspective.

Confidentiality, integrity, and availability impacts

Vulnerability, power imbalance, and data-subject impact findings

Possible exclusion, discrimination, or unequal outcomes

How transparency, access, correction, objection, restriction, challenge, and redress operate

Remediation speed, recovery implications, and operator capacity

Page 8 — Risk and control record

Use one row per material rights risk in Privora Pro. Summarise only decision-level facts here.

Risk and effect on people	Likelihood	Severity	Existing or planned control	Owner and target date	Residual risk	Evidence reference

Unverified controls and unresolved treatment gaps

Privacy-by-design and default measures

Treatment readiness checks

- ☐ Every material risk has an individual owner
- ☐ Dates are realistic
- ☐ Evidence expectation is named
- ☐ Residual ratings follow control evidence
- ☐ Accepted risk has authorised rationale

Page 9 — Transfer and rights review

Does a cross-border transfer apply?

☐ Yes
☐ No
☐ Unconfirmed

Jurisdictions, basis, safeguards, onward transfer, rights, redress, and unresolved issues

Authentication, accessibility, channel, or operational barriers to rights

Page 10 — Decision and conditions

The options are go ahead, modify, or stop. Record what the choice authorises and what it does not.

Recommended final decision

☐ Go ahead
☐ Modify
☐ Stop

Evidence-based rationale for the decision

Conditions, dependencies, interim restrictions, and monitoring owners

Unresolved problems carried to escalation or review

Page 11 — Prior consultation record

Complete only through the organisation's authorised regulatory process. Privora does not create a filing receipt.

Does high residual risk require prior NDPC consultation?

☐ Yes

☐ No

☐ Qualified review pending

Reviewed material, questions, authority, and approved submission route

Authentic consultation date

Authentic outcome and reference, recorded only after receipt

Section 28(2), official PDF p. A735

Page 12 — Sign-off readiness

The certified DPO performs formal vetting in the controlled workflow. This workbook records preparation, not approval. The product's application sign-off is not a cryptographic signature or evidence of regulator endorsement.

Certified-DPO review pack readiness

- ☐ Scope and sources complete
- ☐ Risks and treatment reviewable
- ☐ Decision and conditions recorded
- ☐ Consultation complete where required
- ☐ Draft status is clear
- ☐ Exceptions are visible

Planned or completed certified-DPO review date

Privora Pro review or comments reference

Current controlled state

- ☐ Draft
- ☐ In review
- ☐ Changes required
- ☐ Approved in Privora Pro
- ☐ Stopped

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

Page 13 — Review and lessons

Planned review frequency

☐ Monthly
☐ Bimonthly
☐ Quarterly
☐ Biannual
☐ Annual
☐ Biennial
☐ Lifecycle
☐ Custom

Changes or events that require earlier review

What to improve in the next assessment cycle

Operating-record completion

- ☐ Reviewed information entered in Privora Pro
- ☐ Evidence references checked
- ☐ Draft and approved outputs distinguished
- ☐ Activity history retained
- ☐ Next review owner informed

Sources and review boundary

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

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

Privora Pro remains the operating record after the privacy lead and authorised reviewers enter approved information.