Privora

PRIVACY OPERATIONS · PRIVORA PRO · WORKBOOK

Prepare and record an accountable personal data breach response

Prepare owners, timelines, evidence references, risk decisions, communications, remediation, and closure without copying sensitive payloads.

Primary action

Complete the working pages, then update the client breach record.

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 record an accountable personal data breach response

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

This blank workbook structures professional review; it does not make a notification decision, replace incident command, or prove external filing. Confirm current requirements and the facts of the incident with accountable reviewers.

Confidentiality control: Assign a neutral incident reference and restrict this workbook to the response team. Do not place raw incident payloads, credentials, full identity documents, or copied sensitive records in this workbook. Keep live evidence, personal data, forensic material, affected-person lists, and delivery records in approved systems. Use safe references here, then enter approved information in the correct Privora Pro client workspace.

Privora Pro remains the operating record after approved information is entered. This workbook is a preparation and review aid. Destroy or retain completed working copies according to the organization's authorized incident and records procedure.

Working-page controls

Record the workbook owner, current review state, and permitted audience. Use one version at a time. Mark estimates and disagreements clearly. Do not turn an empty field into a guessed answer merely to make the pack appear complete.

Neutral incident reference

Workbook owner and role

Current review date

Approved confidentiality classification

- ☐ Restricted
- ☐ Confidential
- ☐ Internal

Safe incident command sheet

Name the response authority and the secure systems used for communication and evidence. Do not copy access details into this page. Confirm alternates so urgent work does not stop when one person is unavailable.

Incident lead and alternate

DPO or privacy decision owner and alternate

Security or forensic lead and alternate

Communications owner and approver

Management reviewer with residual-risk authority

Approved secure coordination location reference

Awareness and fact timeline

Separate suspected incident time, discovery time, controller awareness, and later fact changes. State the source for each time in the narrative rather than adjusting dates to match an internal target.

Suspected incident date and time

Initial discovery date and time

Controller awareness date and time

Basis and source for the controller awareness time

Material fact and action timeline with source references

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

Reviewed 2026-08-12 against the linked source material.

Containment and evidence index

Summarize containment and reference evidence without reproducing it. Note whether an action was validated and what risk remains. Preserve provenance and access controls in the evidence repository.

Current containment status

- ☐ Contained
- ☐ Partially contained
- ☐ Not contained
- ☐ Unknown

Containment actions, owners, times, and validation results

Known or credible continuing exposure and escalation

Evidence references, custodians, provenance, and access location

Evidence preservation gaps and recovery owners

Affected people, data, systems, and processors

Use categories and bounded estimates. Never list affected people here. Explain the method and limitations behind each estimate.

Affected-person categories and relevant vulnerability factors

Approximate affected-person count or range

Approximate affected-record count or range

Estimate method, time produced, confidence, and limitations

Affected data categories

- ☐ Identity and contact
- ☐ Financial
- ☐ Authentication
- ☐ Health
- ☐ Biometric
- ☐ Employment
- ☐ Location
- ☐ Communications
- ☐ Children's data
- ☐ Other reviewed category

Affected systems, processes, environments, and interfaces

Processor or recipient involvement, notices, and outstanding facts

Risk and notification decision record

Record the rights-and-freedoms analysis and the two distinct notification questions. Preserve dissent and reassessment triggers. The product does not decide these questions.

Potential harms to affected individuals

Likelihood, severity, protection, vulnerability, and mitigation factors

Is the breach likely to result in risk to rights and freedoms?

☐ Yes

☐ No

☐ Unresolved pending professional review

Commission-notification decision rationale, evidence, and assumptions

Is the breach likely to result in high risk to affected data subjects?

☐ Yes

☐ No

☐ Unresolved pending professional review

Data-subject communication decision rationale and protective actions

Decision owners, reviewers, approvals, dissent, and times

Facts or events that will trigger reassessment

Communications and phased information

Prepare messages from the approved fact set. Keep drafts clearly labelled and store recipient data elsewhere. The authorized operator remains responsible for external delivery and proof of delivery.

Commission notice preparer, approver, and delivery operator

Unavailable notice details, owners, and expected availability

Phased update sequence and without-undue-delay follow-up control

Immediate data-subject communication audience, channel, language, and mitigation advice

Approved version, audience, delivery time, channel, and evidence reference

Remediation and residual risk

Track durable correction separately from immediate containment. Require evidence and reviewer acceptance before marking an item complete.

Remediation actions, accountable owners, dates, dependencies, and status

Remediation validation method, result, period, and evidence reference

Residual risk disposition

- ☐ Accepted by authorized reviewer
- ☐ Further treatment required
- ☐ Blocked and escalated

Monitoring signals, owners, duration, and escalation thresholds

Closure and lessons

Confirm that decisions, communications, external evidence, open actions, and lessons are reconciled before closure. A stopped timer is not closure evidence.

Closure readiness checks

- ☐ Facts reconciled
- ☐ Decisions approved
- ☐ Communications evidenced
- ☐ Sensitive records secured
- ☐ Open actions assigned
- ☐ Residual risk reviewed
- ☐ History preserved

Incident closure decision

- ☐ Close
- ☐ Remain open
- ☐ Close response with tracked remediation

What helped, what delayed work, and what must change

Next remediation or lessons review date

Owner for entering approved records in Privora Pro

Transfer and sign-off

Before transferring the working pack, confirm the correct tenant and client, remove unnecessary personal data, resolve contradictory entries, and retain only the approved operating summary. Generated notices remain drafts until reviewed and approved. Verify external delivery separately before recording submission status or a regulator reference.

Open the client breach register · Privora Pro console

Review response deadlines

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

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

Reviewer sign-off should confirm factual sufficiency, regulatory analysis, communication authority, external delivery evidence, and safe records handling. Escalate unresolved duties or disputed facts for qualified professional review.