

REDDPO PRODUCT FAMILY

DPO Platform

The operational workspace for Data Protection Officers—consent, rights, RoPA, breaches, discovery, and privacy assurance—unified for teams that oversee personal data and AI systems.

One hub. Evidence-ready processes. Companion discovery services. Built for GDPR operations where AI and personal data meet.

1

unified DPO hub

5+

privacy assurance packs

4

discovery microservices

159+

seeded obligations

Why organisations choose the DPO Platform

Privacy teams are asked to prove control—not just write policies. The DPO Platform turns statutory duties into day-to-day operations: structured workflows, subject-facing portals, discovery tooling, and exportable assurance evidence in a single Redmine-based stack.

The problem we solve

- **Fragmented tools** — consents in one system, breaches in spreadsheets, RoPA in documents.
- **AI + personal data** — inventories, DPIAs, and monitoring rarely stay linked.
- **Subject rights pressure** — DSARs and preference changes need portals and audit trails.
- **Evidence for auditors** — reviewers expect signed programmes, not ad-hoc folders.
- **Discovery gaps** — teams cannot answer “where is this person’s data?” without scanners.

What you get

Operate Run consent, RoPA, breaches, and records with status-driven workflows and roles.	Engage Public portal for DSAR, breach reports, and feedback—without full staff accounts.
Discover Find, classify, and redact personal data across sources and documents.	Assure Execute GDPR, DPIA, FRIA, TR 27563, and breach-notification programmes with packs.

Built for real DPO workflows

From a new processing activity to a 72-hour breach clock, the platform connects intake → investigation → decision → evidence. Optional AI system inventory and log analysis keep privacy controls aligned with systems that actually process data.

Platform capabilities

A modular suite under one DPO hub. Enable what you need; keep companion discovery services internal with API keys and network controls.

DPO Hub Organisation and project dashboards with live links to every privacy module and service status.	Consent Library Purposes, PII categories, services, encrypted data subjects, consents, capture API, DSAR export, and governed erasure.
Consent Portal Self-service preference changes with identity matching and staff approve/reject queues.	Public Rights Portal External DSAR, breach reports, incidents, and feedback with optional anonymous intake.
Breach Operations Seven-step breach workflow plus operational monitoring records, SLAs, and CAPA-style evidence.	RoPA Builder Status-driven Record of Processing fields—from responsible parties to transparency obligations.
Records Management File plan, retention, disposal workflow, litigation holds, and permanent disposal log.	Privacy Assurance Packs GDPR, DPIA, FRIA, ISO/IEC TR 27563 privacy, and breach-notification programmes with sign-off.
Assurance Platform Versioned programmes, fieldwork executions, independence guards, plans, and evidence packs.	Regulatory Register Seeded obligations across GDPR, EU AI Act, NIS2, DORA, CRA—and compliance scoring.
System Inventory Register AI/processing systems; link monitoring, portal cases, and assurance executions.	Site Privacy Controls Cookie banner and privacy notice aligned with GDPR/PECR-style expectations.
Personal Information Discovery Multi-source search, DSAR packaging, document scan, and permanent PDF redaction.	pdata-detector Detect personal-data categories in text and structured payloads with tunable rules.
Context Privacy Engine Flag contextual-integrity risks across personal, health, financial, and work contexts.	Runtime Analyzer (optional) Ingest AI logs, detect drift/anomalies, human oversight queue, and Redmine alerts.

Outcomes for your privacy programme

Faster rights fulfilment	Portals, search, packaging, and redaction reduce manual DSAR effort.
Defensible breach response	Timed steps, monitoring records, and notification assurance packs.
Living RoPA & records	Workflow-guided processing records and retention-controlled evidence stores.
Audit-ready assurance	Scored programmes, independence checks, signatures, and exportable packs.
AI-aware privacy	System inventory links consent, monitoring, and assessments to real systems.
One operational home	DPO hub navigation so teams stop hunting across disconnected tools.

How teams use it day to day

New processing: RoPA steps → link system → DPIA/FRIA → consent purposes → file evidence.

Subject request: Portal intake → staff triage → PID search/package → DSAR export → close.

Breach: Detect → structured steps & SLAs → notify → remediate → assurance evidence.

Audit cycle: Select programme → execute fieldwork → review/sign → export pack → dashboard rollup.

Deployment snapshot

Docker Compose project **reddpo** · Redmine core on port **8097** · MariaDB · companion services for discovery, detection, and context checks · safe database export/import with checksums and pre-import safety dumps · role-based access throughout.

Ready to run privacy as an operation—not a binder?

Open the DPO hub after deploy · Explore modules with your privacy team · See the full feature catalogue in [docs/DPO_Platform_Features.md](#)

Local hub: <http://127.0.0.1:8097/dpo> · Portal: <http://127.0.0.1:8097/portal>

This brochure summarises capabilities of the reddpo DPO Platform stack. Feature availability depends on enabled modules, configuration, and deployment. Not legal advice—map controls to your controller/processor obligations with counsel.