Baseel Harrier

Baseel
Security - Technology - Transformation

Find the personal data. Show how you control it.

Baseel Harrier Platform is privacy management software for mid-sized and large enterprises. It finds personal data across your systems, records how it's processed, assesses the risk and helps you evidence each step against privacy frameworks worldwide.

GDPR (EU) | DPDP (India) | PDPL (Saudi Arabia, UAE, Bahrain, Qatar and other jurisdictions) | Additional privacy frameworks worldwide

8	14	4	Full
modules — one suite, or licensed individually	built-in roles, including read-only auditor	deployment options — multi-tenant SaaS, dedicated single-tenant, customer's own cloud or on-premises	audit trail, with each write action attributed to a named user

HOW THE PLATFORM WORKS

01 **Connect**
Register a source. Credentials encrypted, mutual TLS supported.

02 **Scan & profile**
Column-level inventory with per-task scan detail.

03 **Classify**
Personal and sensitive categories, with rule and confidence.

04 **Review & certify**
Reviewers can override; both results are kept. Owners certify.

05 **Record**
ROPA records on versioned, assignable templates.

06 **Assess**
DPIA screening decides what needs full assessment.

07 **Respond**
DSARs and breaches run to statutory deadlines.

08 **Evidence**
Every write action attributed, success or failure.

One foundation for every module: one organisation boundary, user directory, role model, entitlement model and audit trail.

M01 Data Discovery

Establish what your systems actually hold.

- **Connect and scan** databases, warehouses, storage, SaaS, BI, pipelines and file uploads.
- **Profile and classify** into 11 personal-data categories, with rule and confidence.
- **Trust and certification** — an itemised trust score, certified by a named owner.
- **Lineage and impact** — column-level lineage from foreign keys and SQL, traced up to 10 levels deep.

Outcome Discovery gives teams clear visibility into their data and the evidence needed for ROPA, DPIA and risk work.

M02 ROPA

Maintain a defensible processing register.

- **Global privacy requirements** — purpose, legal basis, data categories, recipients, retention, and transfers.
- **Versioned, never overwritten**, so old records stay interpretable.
- **Named ownership** — a data owner on every record, with an optional steward.
- **Country adequacy register** — transfers checked against a maintained adequacy position.

Outcome Processing activities are clearly documented, with a named owner, legal basis and a traceable history of changes.

M03 DPIA

Assess the processing that warrants it — and only that.

- **Configurable screening** — a scored risk model decides whether a full DPIA is needed.
- **Template-driven assessment** with repeatable sections, assigned contributors and inline comments.
- **Legal and IT security input** — each function completes only its own section.
- **DPO review gate** and owner sign-off before go-live; international transfers reviewed separately.

Outcome DPIA decisions and approvals are clearly recorded, with accountability assigned to the right people.

M04 DSAR

Answer data subjects inside the statutory window.

- **Core data subject rights** — access, rectification, erasure, restriction, portability, objection, consent withdrawal.
- **Public intake and verification** — identity verified before any data is assembled.
- **Routed and signed off** by data owner, legal and DPO, then a documented response.
- **SLA tracking** with warnings and escalation; requesters follow a public status view.

Outcome Every request is tracked from start to finish, with clear ownership, deadlines and a complete audit trail.

M05 Breach Management

Decide notification with the facts in front of you.

- **Configurable template** for capturing incidents.
- **Root-cause analysis** — IT security, legal and privacy each own their section.
- **DPO decision gate** — the record cannot close without a notification decision.
- **Regulator notification** generated from the record; SLA timers on the notification window.

Outcome Notification decisions are made on time and on the facts, with a clear record of who decided and why.

M06 Vendor Assessment

Assess third parties before they process anything.

- **Tokenised portal** — vendors answer through a secure link, no account needed.
- **Internal review routing** to the right reviewers; procurement holds final approval.
- **Revision history** — every resubmission kept as a new revision.
- **Evidence retained** — questionnaire, answers and decisions all kept.

Outcome Third parties are vetted before they handle personal data, and any concerns are tracked to resolution in the risk register.

M07 Risk Management

Keep a register that reflects what the assessments found.

- **Raised or escalated** directly, or from ROPA, DPIA and vendor work.
- **Owner, severity, mitigation** and tasks on every risk.
- **Closure needs approval** — owners request closure, the DPO approves it.
- **Remediation tasks** on a Kanban board; overdue tasks flagged.

Outcome Better risk visibility, clear ownership and timely resolution through regular reviews and approvals.

M08 Policy Management

Evidence that each policy was published — and read.

- **Defined lifecycle** — draft, review, approve, publish, retire.
- **Configurable approval chains**; returns go to the step that needs work.
- **Attestation campaigns** with acknowledgement tracking and escalation reminders.
- **Version history** shows which version each person attested to.

Outcome Staff acknowledgements are on record for each policy version, so you can show auditors who has read what.

DATA SOURCES & INTEGRATION

Databases
PostgreSQL, MySQL, MariaDB, SQL Server, Oracle, SQLite

Warehouses
Snowflake, BigQuery, Databricks, Redshift

Storage
Amazon S3, MinIO, Azure Blob, Google Cloud Storage

SaaS apps
Salesforce, HubSpot, ServiceNow, Jira

BI & analytics
Power BI, Tableau, Looker

Pipelines & upload
Apache Airflow, dbt; CSV, Excel, PDF

Extensible connector framework. Also: REST API, lineage export (CSV) and a customer-configured LLM endpoint.

SECURITY CONTROLS

Tenant isolation	Membership and module licence checked centrally on every request.
Access control	14 built-in roles; owners see only their assets; auditors read-only.
Encryption	Data encrypted in transit (TLS) and at rest; credentials and keys additionally encrypted; mutual TLS supported.
Audit trail	Every write action recorded against its user, success or failure.
Minimisation	Frequent values withheld where they would expose personal data.
AI transparency	Every AI interaction kept as a full trace; you configure the model endpoint.

DEPLOYMENT & LICENSING

Licensing	One integrated suite, or any module on its own — add more later.
Structure	Multi-department and multi-team support as standard.
Deployment	Multi-tenant SaaS, dedicated single-tenant, customer's own cloud or on-premises; container image with versioned migrations.
External users	Vendors and data subjects need no account or seat.

USE CASES

Record-keeping	A defensible processing register.
Data mapping	Find personal data across your systems.
DSAR response	Rights requests tracked against statutory deadlines.
Breaches	Decide and notify within 72 hours.
Vendor checks	Assess processors before onboarding.
Audit readiness	Show who decided what, and when.

Who uses it: DPOs, data owners and stewards, legal, IT security, procurement, HR, employees, admins and auditors — with vendors and data subjects reached through secure links. Built for mid-sized and large enterprises.

See it with your own data model.

Vendor Baseel Partners LLP
Website www.baseel.com
Email contactus@baseel.com
Phone +44 20 4540 0111
Address 167–169 Great Portland Street, London W1W 5PF