Baseel Harrier

Baseel
Security - Technology - Transformation

GDPR (EU) · DPDP (INDIA) · PDPL (SAUDI ARABIA, UAE, BAHRAIN, QATAR & OTHERS) · ADDITIONAL FRAMEWORKS WORLDWIDE

Find the personal data. Show how you control it.

Baseel Harrier Platform — privacy management software for mid-sized and large enterprises that finds personal data, records how it's processed, assesses the risk and helps you evidence each step.

Baseel Partners LLP · contactus@baseel.com

THE PROBLEM

The register says one thing. The databases say another.

Privacy laws require organisations to evidence five obligations — yet most still run them on spreadsheets, email threads and disconnected tools.

Keep records

of how personal data is used

Assess risk

before high-risk processing starts

Answer people

who ask about their data

Report breaches

to regulators within 72 hours

Control vendors

who process data on your behalf

THE PLATFORM

Evidence underneath, governance on top.

GOVERNANCE MODULES — record, assess, respond and evidence

ROPA	DPIA	DSAR	Breach Management	Vendor Assessment	Risk Management	Policy Management

Data Discovery — Evidence from your systems: inventory, classification, trust and lineage

Shared foundation — One organisation boundary · user directory · role model · entitlements · audit trail

HOW IT WORKS

From connected source to evidenced decision.

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 and both results are kept; owners certify.

05

Record

ROPA records on versioned, assignable templates.

06

Assess

DPIA screening decides what needs a full assessment.

07

Respond

DSARs and breaches run to statutory deadlines.

08

Evidence

Every write action attributed, success or failure.

MODULE 01 · DATA DISCOVERY

Establish what your systems actually hold.

Multiple connectors

Databases to BI tools, plus file upload.

Secure connections

Credentials encrypted; mutual TLS certificates.

Scan tasks

Run per source, with per-task scan detail.

Column profiling

Statistics and patterns for every column.

Minimised samples

Frequent values withheld where they expose data.

Dashboard & coverage

Live KPIs and a coverage report per source.

SOURCE FAMILIES

- Databases & warehouses
- Cloud & object storage
- SaaS applications
- BI, analytics & pipelines
- **CSV, Excel & PDF upload**

The connector framework is extensible as the estate grows.

MODULE 01 · DATA DISCOVERY

Classification you can argue with.

11 categories

Email, name, phone, credentials and more.

Shown its working

Method, rule, confidence, and if AI was used.

Reviewer override

Corrections kept beside the original result.

Trust & certification

Itemised trust score; a named owner certifies.

Lineage & impact

From keys and SQL, up to 10 levels; CSV export.

Ask AI

Question the catalogue; every exchange traced.

FROM COLUMN TO EVIDENCE

- Profiled column
- Classified · rule + confidence
- Reviewed · override kept
- Trust checks scored
- **Certified by a named owner**

Analysts check ROPA and DPIA records against this verified inventory.

MODULE 02 · ROPA

A defensible processing register.

Processing register fields

Purpose, legal basis, recipients, retention, transfers.

Flexible templates

8 field types, dynamic options, validation rules.

Named ownership

A Data Owner and Data Steward on every assignment.

Cross-border routing

Transfers go to Legal's queue automatically.

Raise a risk

From any record, linked into the risk register.

Export

Selected records or the full register, for reporting.

RECORD LIFECYCLE

Draft

Submitted

Pending review (DPO)

Approved — or rejected with comment

Every review cycle increments a revision number, so the full history stays reproducible.

MODULE 03 · DPIA

Assess what warrants it — and only that.

14-question screening

Calculates a Low, Medium or High risk band.

Sections unlock

Medium or High opens the full assessment.

DPO override

“Require full DPIA” on any Low result.

Legal & IT security

Each edits only its own sections and comments.

Risk scoring

Likelihood × Impact, 1–25, plus residual risk.

Repeatable sections

“Add another” for multi-system projects.

ASSESSMENT LIFECYCLE

- Draft
- Screening complete · band set
- Submitted → pending DPO review
- Approved
- **Final approved**

Only the DPO approves. Every decision is recorded against a person.

MODULE 04 · DSAR

Answer every request inside the window.

Core data subject rights

Access to consent withdrawal, one workflow.

Public portal

Requests by web form or email, no account.

Identity checks

5 methods, Low to High assurance.

30-day SLA

Documented extensions; DPO alerted before breach.

Stage templates

Six configurable forms, intake to legal review.

Closure evidence

Closure PDF and a full case timeline.

CASE ROUTE · DSR-YYYY-NNN

- Open · SLA clock starts
- DPO review & identity verified
- Legal review & redactions
- Data Owner compiles data
- **DPO sign-off · closed**

Invalid jumps are rejected; every change is logged.

MODULE 05 · BREACH MANAGEMENT

Seventy-two hours, tracked from discovery.

Alert to incident

Anyone raises an alert; an admin registers it.

Impact scoring

Sensitivity × scale, 1–25, in four bands.

Legal gate

Legal recommends; the DPO approves or overrides.

SLA alerts

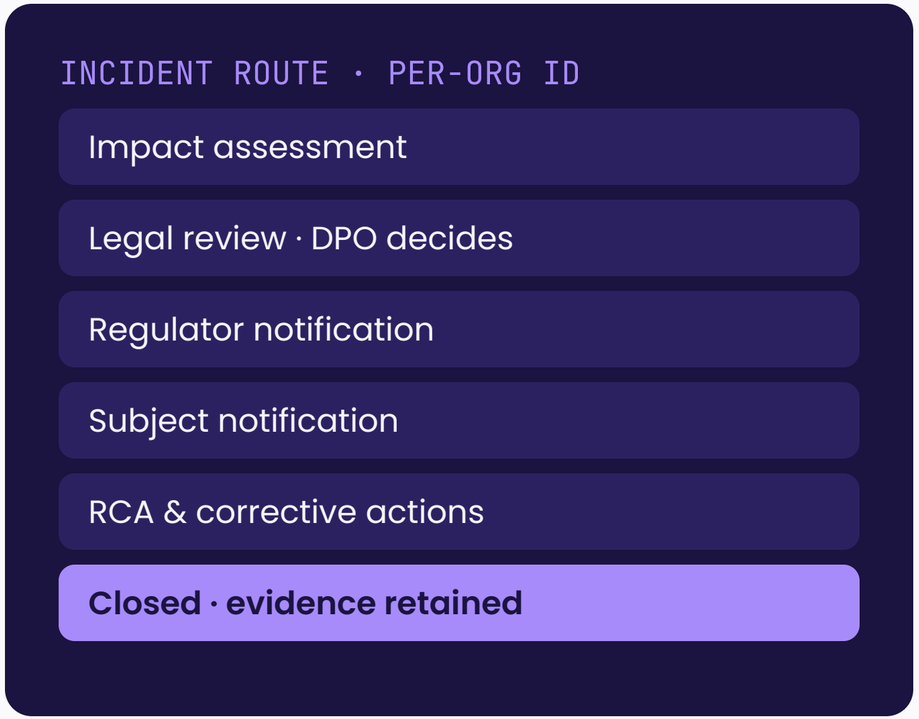
Warnings at 48 and 60 hours; breach flagged at 72.

Notification

Regulator notice and logged subject emails.

RCA & CAPA

IT submits; the Data Owner must acknowledge.



MODULE 06 · VENDOR ASSESSMENT

Assess third parties without giving them a seat.

Secure form link

Time-limited token by email; no login needed.

Email verification

A 6-digit code before the form opens.

Autosave & files

Progress saved; attachments supported.

Two-stage review

Internal reviewers, then Procurement decides.

Flag risk per answer

Concerns go straight into the risk register.

Assessment PDF

A summary for onboarding and audit files.

RESPONSE LIFECYCLE

- Pending
- Submitted
- Under internal review
- Approved internally
- **Final decision · Procurement**

Rejected responses go back to the vendor; each resubmission is a new revision.

MODULE 07 · RISK MANAGEMENT

Every privacy risk, in one register.

Raised at the source

From ROPA, DPIA or vendor answers, linked back.

Direct logging

Data Stewards log risks across 8 categories.

Severity scoring

Likelihood × impact, scored automatically.

Mitigation plans

Mitigate, transfer, accept or avoid — with dates.

Remediation tasks

Kanban for owners; overdue tasks flagged.

DPO closure

Owners request closure; the DPO decides.

SEVERITY BANDS · L × I

- 1–4 · Low
- 5–9 · Medium
- 10–15 · High
- **16–25 · Critical**

A risk from another module shows the exact question and answer that raised it.

MODULE 08 · POLICY MANAGEMENT

Publish a policy — and prove it was read.

Policies & procedures

Two document types, one governance layer.

Two authoring modes

Structured template, or upload Word or PDF.

Approval chains

Any one, all required, or strict sequence.

Version snapshots

Every draft and submission is preserved.

Attestation campaigns

All staff, by role, or a custom audience.

Evidence export

Trail, versions, approvals and attestations.

DOCUMENT LIFECYCLE

Draft · collaborative sections

Review · approval chain

Approved

Published · attestation

Retired documents keep their history. Review due: policies 12 months, procedures 6.

TRACEABILITY

Every decision has a name and a time.

Append-only audit trail

Every write action, success or failure.

Versioned records

ROPA revisions, policy snapshots, vendor rounds.

Linked risks

Each risk points to the answer that raised it.

Evidence exports

DSAR closure PDF, breach and policy packs.

Full of write actions attributed to a named user.

AUDIT ENTRY

```
actor dpo@org
action LEGAL_GATE_FINALISE
step LEGAL_REVIEW
status PENDING → FINALIZED
at 2026-10-29 09:14:07Z
```

Rows are inserted, never updated or deleted.

ROLES & ACCESS

Every role scoped to its job.

PLATFORM

- Super Admin
- Tech Admin
- Org Admin

PRIVACY & LEGAL

- DPO
- Legal Team

DATA & SECURITY

- Data Owner
- Data Steward
- IT Security

BUSINESS

- HR
- Procurement
- Auditor
- Employee

EXTERNAL

- Vendor
- Data Subject

Enforced at the API
Hiding a button is not access control.

Owners see their own
Assets are scoped to the people who hold them.

Auditors read-only
Full visibility, no ability to change.

SECURITY

The controls a security review will ask about.

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.

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 set the model endpoint.

DATA SOURCES & INTEGRATION

Connect the estate you already run.

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

Also Extensible connector framework · REST API · lineage export (CSV) · customer-configured LLM endpoint

DEPLOYMENT & LICENSING

License what you need. Run it where you need it.

Licensing

One integrated suite, or any module alone — add more later.

Structure

Multi-department and multi-team as standard.

Deployment

Multi-tenant SaaS, dedicated single-tenant, customer’s own cloud or on-premises.

External users

Vendors and data subjects need no seat.

DEPLOYMENT OPTIONS

- Multi-tenant SaaS
- Dedicated single-tenant
- Customer’s own cloud
- On-premises
- **Container image · versioned migrations**

REGULATORY COVERAGE

Mapped to the duties regulators actually check.

DUTY	MODULE	GDPR REFERENCE
Keep a record of processing	ROPA	GDPR Art. 30
Assess high-risk processing	DPIA	GDPR Art. 35
Honour data subject rights	DSAR	GDPR Arts. 15–22
Notify personal data breaches	Breach	GDPR Arts. 33–34
Govern processors and vendors	Vendor	GDPR Art. 28
Demonstrate accountability	Policy · Risk	GDPR Arts. 5(2), 24

The same workflows cover equivalent duties under India’s DPDP Act, the PDPLs of Saudi Arabia, the UAE, Bahrain, Qatar and other jurisdictions, and additional privacy frameworks worldwide.

Baseel Harrier

Baseel
Security - Technology - Transformation

NEXT STEP

See it with your own data.

EMAIL
contactus@baseel.com

PHONE
+44 20 4540 0111

WEBSITE
www.baseel.com

ADDRESS
Baseel Partners LLP · 167–169 Great Portland Street, London W1W 5PF