THE RiskaVaire OPERATIONALIZES PRIVACY REVOLUTION

Privacy by Design, Governance by Default — how RiskaVaire embeds privacy across the enterprise.

Privacy isn’t an add-on; it must be built into controls, processes, data flows, and vendor ties, directly linked to business risk and value. Vardaan’s GRC platform, RiskaVaire, transforms privacy obligations into operational strength and stakeholder trust

1. Unified privacy controls, a single source of truth for obligations

What it is: a centralized control library that normalizes requirements from GDPR, CCPA, LGPD, HIPAA, ISO 27701 and industry rules into actionable, reusable controls.

How RiskaVaire implements it (deep):

Control taxonomy & attributes:

Each control has type (technical/ administrative/ physical), owner, frequency, evidence attachments, maturity rating, mapped legal clauses, and test procedures.

Cross-framework crosswalks:

obligations that look different across regulations are reconciled to one canonical control (e.g., consent management across GDPR & CCPA becomes a single consent-control with framework-specific parameters)

Inheritance & scope rules:

Policies and controls can be inherited across business units and geographies with override rules for local variance, so global standards coexist with local adaptations.

Control templates & playbooks:

Pre-built templates for common privacy controls (consent, retention, pseudonymization, access control) plus playbooks for implementation and evidence collection.

Outcome:

Consistent control implementation, faster audits, and reduced duplication of effort across regulatory regimes.

How RiskaVaire implements it (deep):

DPIA orchestration: guided questionnaires that adapt to context (data types, processing purpose, risk level). The platform calculates risk scores and recommends mitigation actions (encryption, retention changes, contract clauses).

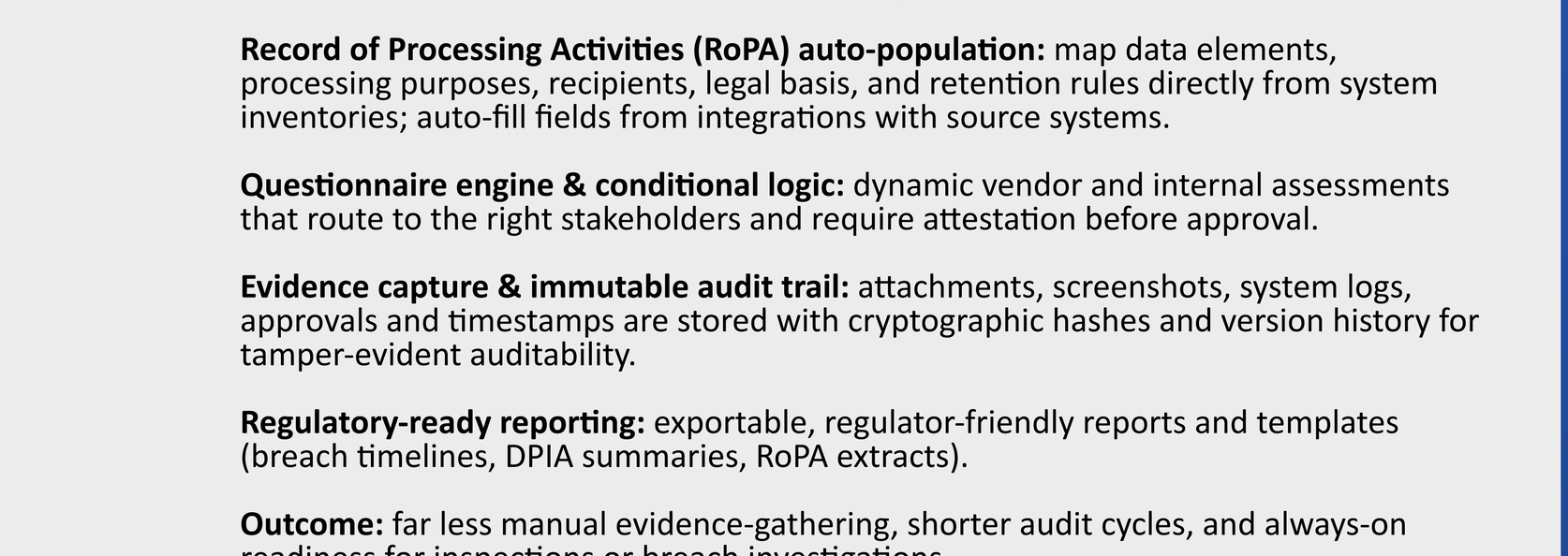
Record of Processing Activities (RoPA) auto-population: map data elements, processing purposes, recipients, legal basis, and retention rules directly from system inventories; auto-fill fields from integrations with source systems.

Questionnaire engine & conditional logic: dynamic vendor and internal assessments that route to the right stakeholders and require attestation before approval.

Evidence capture & immutable audit trail: attachments, screenshots, system logs, approvals and timestamps are stored with cryptographic hashes and version history for tamper-evident auditability.

Regulatory-ready reporting: exportable, regulator-friendly reports and templates (breach timelines, DPIA summaries, RoPA extracts).

Outcome: far less manual evidence-gathering, shorter audit cycles, and always-on readiness for inspections or breach investigations.



2. Automated assessments & documentation, evidence without the paperwork backlog

What it is: automated workflows to run DPIAs, populate RoPAs, perform vendor privacy questionnaires, and capture versioned evidence.

3. Data flow & vendor risk mapping, see where data lives and who touches it

What it is: discovery, classification and lineage that show data movement across systems, teams and third parties.

How RiskaVaire implements it (deep):

Automated Discovery Connectors:

Ingest Metadata From Cloud Storage, Databases, SaaS Apps, Message Queues And Data Lakes To Find Personal Data Hotspots

Data Classification & Tagging:

Apply Standardized Classification (PII, PHI, Sensitive, Internal) And Tag With Business Context (Purpose, Retention, Legal Basis).

Lineage & Flow Visualizations:

Graphical Maps That Show Origin → Transformation → Destination (Including Third-Party Transfers), With Clickable Nodes For Controls, Contracts And DPIAs.

Third-Party Risk Management (TPRM):

Vendor Inventory Linked To Data Flows; Vendor Assessments, Contract Clause Tracking (BAA, SCCs), Certificate Expirations And Remediation Workflows

Cross-Border Transfer Tracking:

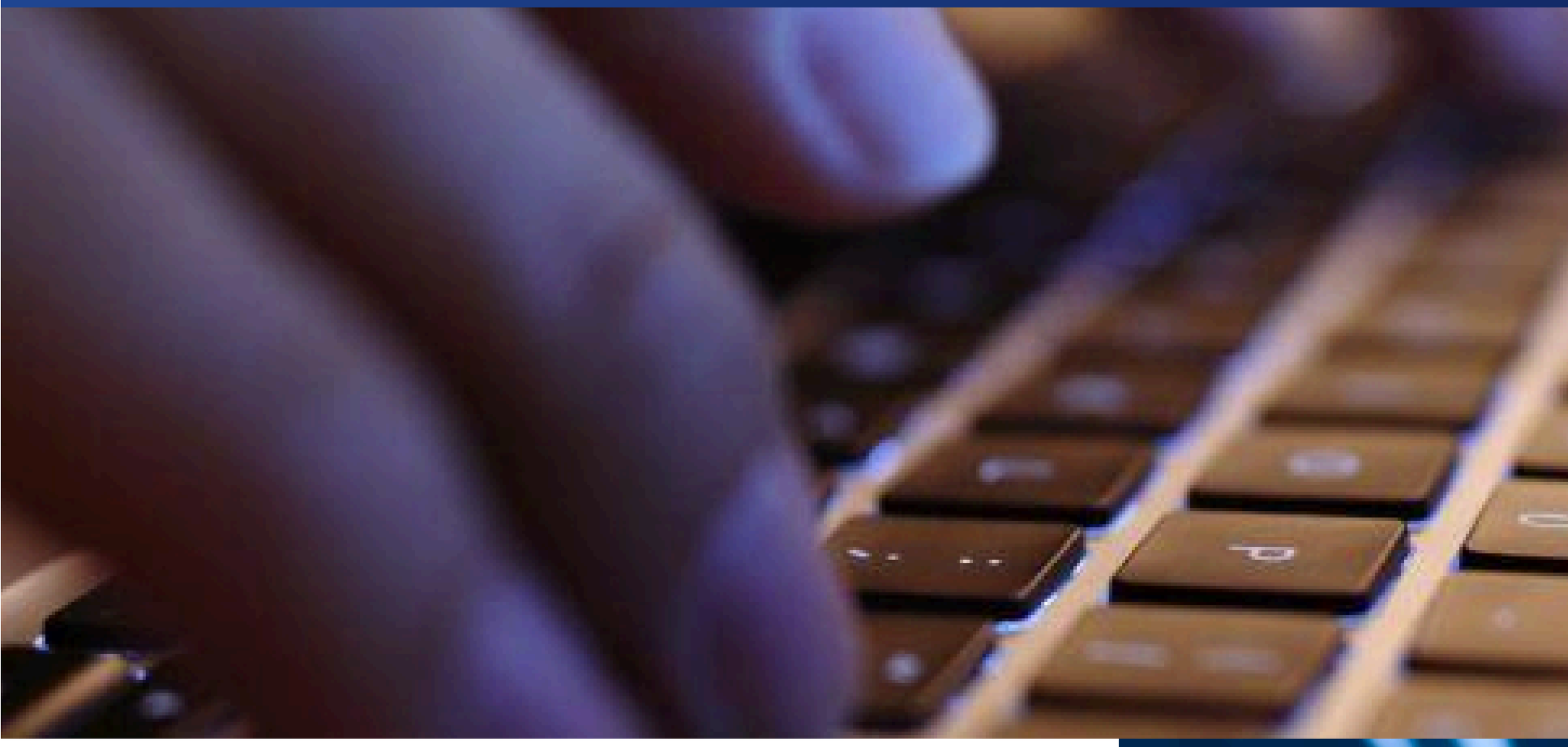
Flag Transfers To Jurisdictions With Restrictions And Surface Required Protections (SCC, DPA, Adequacy Decisions).

Outcome:

The Organization Tracks Personal Data Flow And Vendor Scope, Enabling Faster Incident Response And Stronger Risk Management.

What it is: discovery, classification and lineage that show data movement across systems, teams and third parties.

- Integration fabric: plug into SIEM, DLP, IAM, CASB, cloud audit logs and application telemetry to surface privacy-relevant incidents (unusual exports, mass downloads, privilege escalations).
- Integration fabric: plug into SIEM, DLP, IAM, CASB, cloud audit logs and application telemetry to surface privacy-relevant incidents (unusual exports, mass downloads, privilege escalations).
- Anomaly detection & predictive signals: behavioural baselining to detect exfiltration patterns, spikes in DSARs, or unusual vendor activity. (Optionally augmented with ML models.)
- Continuous control testing: scheduled checks of encryption, access policies, retention deletes and backup protections with automated reporting on failures.
- Outcome: risk is discovered early, workflows start automatically, and human attention is reserved for decisions rather than detection.



5. Continuous monitoring & alerts, detect, not just document

What it is: real-time (or near real-time) monitoring of privacy control health and anomalous events with automated escalation and remediation options.

How RiskaVaire implements it (deep):

Integration fabric: plug into SIEM, DLP, IAM, CASB, cloud audit logs and application telemetry to surface privacy-relevant incidents (unusual exports, mass downloads, privilege escalations).

Policy-based alerting: thresholds and rules that trigger workflows (e.g., >X records exported from CRM within Y minutes triggers a ticket and suspends the account).

Anomaly detection & predictive signals: behavioural baselining to detect exfiltration patterns, spikes in DSARs, or unusual vendor activity. (Optionally augmented with ML models.)

Integration fabric: plug into SIEM, DLP, IAM, CASB, cloud audit logs and application telemetry to surface privacy-relevant incidents (unusual exports, mass downloads, privilege escalations).

Integration fabric: plug into SIEM, DLP, IAM, CASB, cloud audit logs and application telemetry to surface privacy-relevant incidents (unusual exports, mass downloads, privilege escalations).

6.Alignment with governance & risk objectives, privacy as part of the risk fabric

What it is: real-time (or near real-time) monitoring of privacy control health and anomalous events with automated escalation and remediation options.

- Risk mapping: link each privacy control to risk statements and business processes, so control gaps show up in enterprise risk dashboards.
- KRI/KPI integration: measure privacy KPIs (DSAR SLA, DPIA completion, % of data assets classified) as KRIs to the board-level risk reports.
- Risk scoring & simulation: combine likelihood and impact, simulate remediation scenarios and show residual risk post-mitigation
- Board & regulator packs: templated, executive-ready reports translating technical controls into business impact (financial exposure, reputational score)..
- Policy & exception governance: manage policy exceptions with approvals, due-dates and compensating controls, ensuring exceptions are visible to governance bodies.
- Outcome: privacy isn’t a silo; it informs strategic decision-making and is evaluated against the same risk appetite as cyber, operational, and financial risks.

7. Privacy as a stakeholder commitment, practical mechanisms to prove trust

What it is: operational features that make the enterprise accountable and transparent to customers, employees, partners and regulators.

Consent lifecycle & preference management: centralize consent records, map consent to processing activities, and honour revocations automatically across systems.

DSAR automation: intake portals, identity verification workflows, automated search across data sources, redaction utilities, and SLA tracking with audit trails.

Privacy notices & contractual templates: manage and version privacy notices; push updates to web properties; maintain contract clause libraries and track sign-offs.

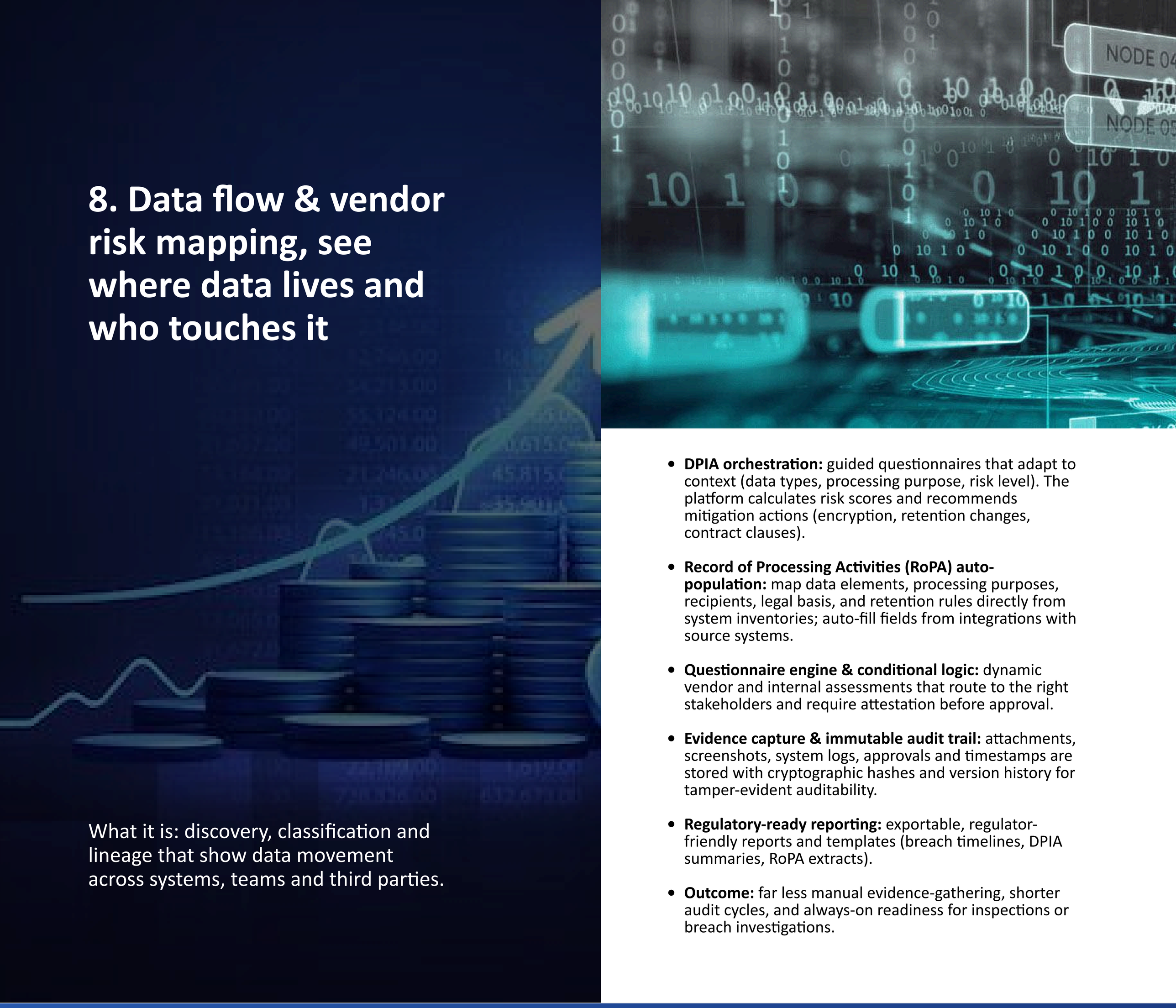
Breach response orchestration: pre-defined playbooks, notification templates, regulator-specific reporting timelines and post-incident root-cause analysis modules.

Training & attestation: automated training assignments for data handlers, attestations logged in the platform and linked to roles and processes.

Transparency logs: accessible logs showing accesses and disclosures for stakeholders where appropriate (for internal audit, customer requests or regulators).

Outcome: the organization demonstrates consistent, documented behaviour that strengthens trust and reduces regulatory friction.

8. Data flow & vendor risk mapping, see where data lives and who touches it



What it is: discovery, classification and lineage that show data movement across systems, teams and third parties.

- **DPIA orchestration:** guided questionnaires that adapt to context (data types, processing purpose, risk level). The platform calculates risk scores and recommends mitigation actions (encryption, retention changes, contract clauses).
- **Record of Processing Activities (RoPA) auto-population:** map data elements, processing purposes, recipients, legal basis, and retention rules directly from system inventories; auto-fill fields from integrations with source systems.
- **Questionnaire engine & conditional logic:** dynamic vendor and internal assessments that route to the right stakeholders and require attestation before approval.
- **Evidence capture & immutable audit trail:** attachments, screenshots, system logs, approvals and timestamps are stored with cryptographic hashes and version history for tamper-evident auditability.
- **Regulatory-ready reporting:** exportable, regulator-friendly reports and templates (breach timelines, DPIA summaries, RoPA extracts).
- **Outcome:** far less manual evidence-gathering, shorter audit cycles, and always-on readiness for inspections or breach investigations.

9. Technical architecture & integrations, plug into your estate

What it is: an API-first, connector-friendly platform that coexists with your security stack.

Connectors & APIs:

Native connectors for IAM, HRIS, CRM, cloud storage, databases, SIEM, DLP and major SaaS apps; developer APIs for custom sources.

Identity-aware controls:

integrate with IAM to map identity risk, apply least-privilege based on role and context, and automate provisioning/de-provisioning.

Encryption & pseudonymization utilities:

manage keys, tokenization, and pseudonymization workflows tied to data classification.

Event-driven workflows:

triggers from logs or sensors start DPIAs, revoke access or open incident tickets automatically.

Secure architecture:

role-based access, audit logging, encryption at rest/in transit, and tenancy/ isolation options for regulated clients.

Outcome:

technical integration makes privacy controls enforceable where the data lives, not just documented in a policy.

Discovery:

RiskaVaire discovers customer PII in CRM and analytics buckets, tags it, and maps the flow to the vendor.

DPIA:

: automated DPIA runs, identifies high risk due to profiling and cross-border transfer; recommends pseudonymization and a contractual SCC for transfers.

Vendor Assessment

TPRM questionnaire triggers; vendor score below threshold; platform routes remediation (encryption, audit right) and holds contractual changes until score improves.

Monitoring:

DLP alert detects large export from analytics; automated playbook suspends export, opens an incident, notifies the DPO, and logs evidence.

Governance:

residual risk is calculated and presented in the board pack with recommended acceptance or mitigation.

Outcome

the new product launches with documented privacy controls, measurable risk reduction, and demonstrable compliance.

10. A pragmatic scenario, how the pieces come together

Example: a retail bank launches a new credit-offer engine that uses CRM, analytics and a third-party credit-scoring vendor.

Losing, Privacy As Strategic Advantage

RiskaVaire treats privacy as an enterprise capability, not a project. By unifying controls, automating evidence, mapping data flows, continuously monitoring, aligning to risk and operationalizing governance, the platform helps organizations turn regulatory obligation into demonstrable, auditable trust.

CONTACT

info@vardaanglobal.com

+91 40-35171118, +91 40-35171119

Aurum, 1st Floor, Plot No 57,
Jayabheri Enclave, Gachibowli
Hyderabad-500032 INDIA

Vardaan Global

MAKE IN INDIA