SOURCE-CODE PRIVACY SCANNING

ACOMPLI

HOW IT WORKS — SIX STAGES

From source code to *governed privacy evidence*

Six stages take a connected repository from pre-scan planning to reviewed findings and onwards to Article 30 records, DPIA triggers, and data map updates — with a human approval gate at the review stage.

00 Connect | 01 Plan | 02 Scan | 03 Review | 04 Sync | 05 Monitor

---

Discover with code. Decide with people. Publish with evidence.

00

Connect repositories without cloning everything locally

Connect GitHub or GitLab repositories through read-only, scoped access. Framework, package, and data-store discovery runs alongside the scan so the platform knows what is actually in the stack — not only what the documentation says.

GITHUB & GITLAB

Scoped, read-only connection

Authorise the repositories you want scanned. A zero-copy API path avoids replicating source to a third environment.

STACK DISCOVERY

Frameworks & packages

Manifests, frameworks, and build context are identified alongside the parse — an inventory of what is running.

DATA STORES

Connection strings & ORM

Database connections and ORM models are discovered so scans know where personal data is persisted.

Connected repositories feed a structured view of the stack, not only a list of fields.

01

Agentic pre-scan planning, approved before the scan runs

Before a scan touches the repository, a planning step reviews the stack and prior scan context to propose a scan plan. The plan is reviewed and approved by a DPO or privacy engineer before execution.

SCOPE PROPOSAL

Languages, paths, files

The planner recommends a scan scope with rationale captured for review and sign-off.

KNOWN ENTITIES

Prior findings surfaced

Existing Knowledge Base entities and prior scan results surface as context for the plan.

DPO APPROVAL

Exclusions logged as evidence

Scope decisions, exclusions, and rationale are recorded as part of the audit trail — not buried in config files.

The approval itself becomes part of the scan record: who approved the plan, when, and on what grounds.

Scope, rationale, and approval recorded before a single line is parsed.

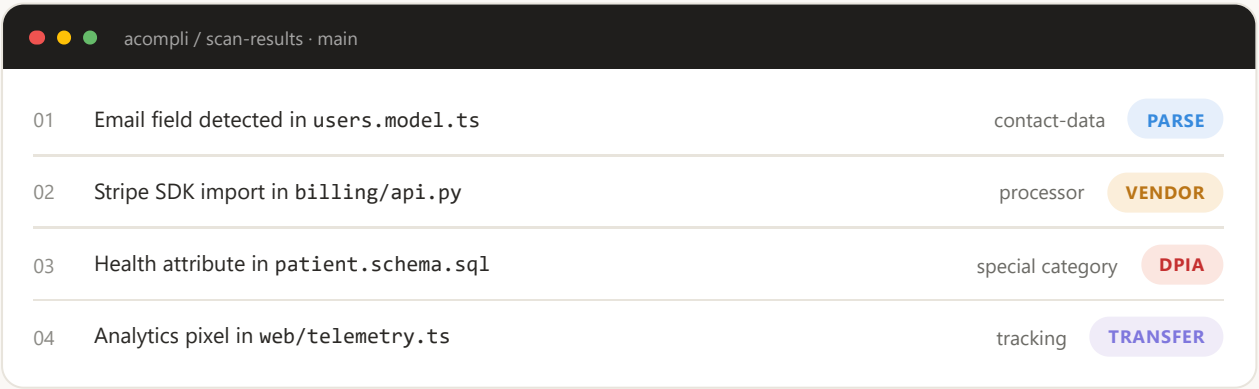
02

Structural source analysis, not keyword search

The scan engine analyses source code structurally across the languages most enterprise codebases are built in. Fields, schemas, SDK imports, and transfer destinations are identified from the parse tree — not from fuzzy keyword matching.

Findings are classified against a deep personal-data taxonomy and matched against a library of vendor and SDK mappings. Each finding carries file, line, and parse-node provenance so reviewers can confirm or reject on the evidence.

10+	68	60+
LANGUAGES PARSED	PII CATEGORIES	VENDOR & SDK MAPPINGS



Every finding carries file, line, and parse-node evidence. No keyword guessing.

03

Human approval on every finding before it becomes a record

Findings land in a review workflow that privacy and engineering share. Reviewers confirm, reject, or annotate each finding with the underlying code visible in context. Nothing is published to the data map, Article 30 record, or DPIA trigger without human approval.

SIDE-BY-SIDE REVIEW

Code in context

Finding and source code shown together, with line-level context for confident decisions.

DPO APPROVAL GATE

Nothing syncs unapproved

Nothing propagates downstream until a reviewer approves. High-risk findings can require dual sign-off.

REVIEWABLE AUDIT TRAIL

Decisions as evidence

Who approved what, when, and on what grounds — review decisions recorded alongside the finding.

AI assists with classification suggestions, vendor mapping, and drafting during review — always as a suggestion a reviewer can accept or reject. The approval gate stays with the human.

Discover with code. Decide with people. Publish with evidence.

04

Approved findings feed data mapping, RoPA, and DPIA evidence

Confirmed findings sync into the Knowledge Base — data nodes, data elements, data flows, linked IT systems, and third-party records. Article 30 drafts are pre-populated with scan evidence attached. DPIA triggers surface when special-category indicators or high-risk transfer patterns are confirmed.

DATA MAPPING

Living data map

Data nodes, elements, and flows sync from reviewed findings. Every node keeps a link back to the source code.

ROPA DRAFTS

Article 30 with scan evidence

Draft processing activities pre-populate from approved findings, with the scan trail attached for review.

DPIA TRIGGERS

High-risk patterns surfaced

Special-category indicators, novel transfers, or vendor risk can mark processing as DPIA-relevant automatically.

EVIDENCE PACKS

One finding, many audiences

SARIF for engineering, PDF for executive review, CSV for audit, compliance reports for regulators.

One finding. Many audiences. Every export points back to the code.

05

Continuous monitoring as the codebase evolves

Connected repositories can be rescanned as code changes. New findings enter the same review workflow; confirmed changes update the data map, RoPA drafts, and DPIA triggers without starting over.

What was approved previously remains auditable. Every rescan preserves the prior decision trail, so the record shows what changed, who approved the change, and which outputs moved in response.

RESCAN ON CHANGE

Same review workflow

Connected repositories can be rescanned as code evolves. Findings enter the same review workflow reviewers already know.

PRESERVED DECISIONS

Auditable across rescans

Prior reviewer decisions remain auditable, with a clear record of what changed and why it changed.

DOWNSTREAM PROPAGATION

Outputs update automatically

Confirmed changes update the data map, RoPA drafts, and DPIA triggers — without re-running the whole process by hand.

ONGOING EVIDENCE

A control, not a project

Privacy-by-design review becomes an ongoing control rather than a one-off assessment.

Privacy evidence that moves with the codebase.

— THE OUTCOME

Privacy evidence from the *code itself*

Six stages, one thread of evidence. Findings come from a deterministic scan, pass through a human approval gate, and land as records the business can stand behind — Article 30 drafts, DPIA triggers, a living data map, and export-ready evidence packs.

DATA MAP

Living & code-linked

Every node traceable back to the source code that produced it.

ARTICLE 30

Pre-populated drafts

Processing activity records with the scan trail already attached.

DPIA

Risk-triggered

Special-category or high-risk transfer patterns flag automatically.

EVIDENCE

Export in every format

SARIF, CSV, PDF, and regulator-ready compliance reports.

Discover with code. Decide with people. Publish with evidence.