EVIDENCE SIGNALS REPORT | FIG. 00 — POSTURE SUMMARY | compliance-as-code assessment

GDPR compliance posture: 30% of requirements implemented across 7 modules.

An evidence-led readout of where this organization stands against GDPR — grouped by obligation, scored by what the agent actually found in code, generated on demand from the live audit trail. **This document is the report.** Re-share the link, export a PDF, or open any module to drill in.

ORGANIZATION	REGULATION	GENERATED	SCAN SESSIONS	REPOSITORIES
org_f296b4ca5f78	GDPR · EU 2016/679	2026-04-29 18:59:10Z	4 · cumulative	api · application · frontend
workspace · acme	7 modules · 118 reqs	build #756a5a7	latest · session_04	3 scanned · 0 skipped

§ 00 · READER'S NOTE

how to read this report

est. 4 min

GDPR is decomposed into **7 modules** of related obligations. Each module contains **118** IT requirements in total, and each requirement has 3–5 **compliance checklist items** (**576** altogether) — the actionable items the AI coding agent searches the codebase for.

A requirement is marked `IMPLEMENTED` when the agent finds code-type evidence at high confidence (≥ `0.7`); `PARTIAL` when it finds something less conclusive; otherwise `GAP`. Numbers labelled **active** below are deduplicated to the most recent scan per requirement-and-repository, so re-scanning the same code never inflates the count. **Cumulative** numbers are the full audit trail across every scan session.

§ 01 / 03

COMPLIANCE POSTURE

How the 118 requirements distribute across implemented, partial, and gap.

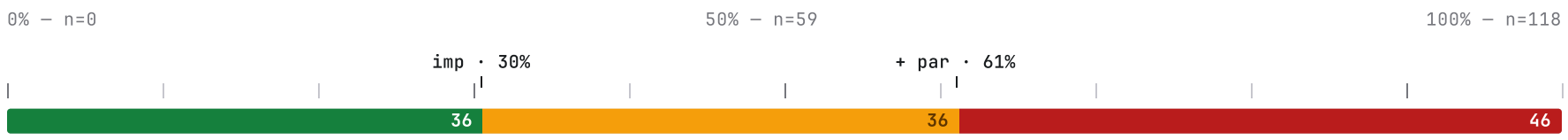
Distribution measured against the full GDPR requirement set in scope (n = 118). Bar segments are proportional; tick marks are at every 10%. Counts are **active** (deduplicated to latest evidence per requirement+repository).

POSTURE INDEX

30%

of **118** requirements implemented at **≥0.7**

`36 implemented` and `36 partial` leave `46 in gap` across the 118-requirement GDPR scope.



IMPLEMENTED	PARTIAL	GAP
30.5%	30.5%	39.0%
36	**36**	**46**
requirements with **code-type** evidence ≥0.7	evidence found but **below threshold**	no signal · **requires action**

§ 02 / 03

SCOPE & EVIDENCE

What was assessed, and what evidence was collected.

Left — the **scope** the assessment ran against. Right — the **evidence** the agent surfaced. The two are independent: scope is fixed by the regulation; evidence grows with every scan.

fig. 02.1 / **scope-of-assessment** — IN-SCOPE · N = 118

Assessed against **7** GDPR modules containing **118** IT requirements and **576** compliance checklist items.

7	118	576
MODULES	IT REQUIREMENTS	CHECKLIST ITEMS
obligation groups	3-5 checks each	agent-actionable

fig. 02.2 / **evidence-collected** — SIGNALS · 4 SESSIONS

303 active evidence signals (deduplicated) — **398** cumulative across the full audit trail, gathered over **4** scan sessions across **3** repositories.

303	398	4	3
ACTIVE	CUMULATIVE	SESSIONS	REPOS
deduplicated	all scans	latest · 04	api · app · fe

§ 03 / 03

MODULE BREAKDOWN

One row per GDPR module.

Implemented + Partial + Gap reconciles to the requirement count for each module. Evidence is shown as **active / cumulative** — re-scans never inflate the active number. Module names are clickable in the live document.

tbl. 03.1 / **modules · n = 7 · sorted by requirement count** — implemented · partial · gap

MODULE	DISTRIBUTION	REQS	IMP	PAR	GAP	ACTIVE	CUMUL.
01 Controller Governance & Accountability		32	9	11	12	78	79
02 Access Control & Security Measures		19	18	1	0	86	181
03 International Transfer Governance		16	0	6	10	34	34
04 Breach & Change Notification Pipeline		16	0	9	7	33	33
05 Data Subject Rights Operations		15	1	9	5	32	32
06 Lawful Basis & Consent Engineering		11	8	0	3	37	37
07 Records, Retention & Minimization		9	0	0	9	3	2
Σ TOTAL		118	36	36	46	303	398

reconciles · **36 + 36 + 46 = 118** — active dedup ratio · **303 / 398 = 76.1%** — continues below · **requirement-level breakdown ↓**

§ 04 / 05

EVIDENCE LIST

Per-requirement evidence signals, grouped by module.

Each row is one requirement. Status pill (**implemented · partial · gap**) reflects the current evidence verdict; risk pill is the requirement's intrinsic risk if unmet. File paths are clickable in the live document and resolve to the latest scanned commit.

MODULE 01 · 32 REQUIREMENTS

9 implemented · 11 partial · 12 gap · 78 active evidence signals

Controller Governance & Accountability

Art. 37

e498d504b666

GAP HIGH RISK

dpo-qualification-assessment-gap — No formal DPO qualification assessment or selection process found in code. privacy@decisionrecords.org is referenced as contact only.

Art. 31

5212478857a0

IMPLEMENTED MODERATE RISK

audit-log-system-implementation — Immutable audit log system for admin/steward actions. `log_admin_action` helper creates entries for high-impact changes.

EVIDENCE FILES · 3 • models.py • ee/docs/breach-notification-procedure.md • privacy.py

Art. 27

8efef4c1c81b

GAP MODERATE RISK

eu-representative-designation-gap — No formal EU representative designation. If EU-based (Azure EU deployment), Art. 27 may not apply. No formal assessment documented.

Art. 38

139a52e399d9

GAP MODERATE RISK

dpo-system-access-provisioning-gap — No DPO-specific access provisioning. Super Admin role has full access and could serve DPO function, but RBAC system (GlobalRole enum) does not include a DPO role.

EVIDENCE FILES · 1 • models.py

Art. 37

719225690805

PARTIAL MODERATE RISK

dpo-contact-details-published — security@decisionrecords.org published in breach procedure, DPA on marketing site, DPIA documents. Missing: formal SA notification of DPO appointment.

EVIDENCE FILES · 1 • ee/marketing/src/app/components/data-processing/data-processing.component.ts

Art. 26

9908346756d1

GAP MODERATE RISK

joint-controller-arrangement-gap — No joint controller arrangement system. Application operates as sole controller. Sub-processor relationships documented but no joint controller scenarios identified.

Art. 24

98d57d222ca2

IMPLEMENTED HIGH RISK

technical-organisational-measures-framework — Comprehensive TOMs: TLS 1.3, AES-256, RBAC+tenant isolation, Key Vault, Cloudflare WAF, NSG firewall, audit logging (40+ types), Secure+HttpOnly cookies, CSRF protection, input sanitization, consent management.

EVIDENCE FILES · 2 • security.py • ee/docs/security.md

Art. 32

8cd38925562c

IMPLEMENTED HIGH RISK

high-impact-settings-guard-implementation — Prevents accidental lockout and restricts high-impact settings based on tenant maturity or multi-admin consensus.

EVIDENCE FILES · 3 • crypto.py • governance.py • ee/docs/dpia/

Art. 32

5093e12a7d88

IMPLEMENTED HIGH RISK

gdpr-compliance-tests-implementation — Comprehensive tests covering erasure, portability, consent management, and automated anonymization tasks.

EVIDENCE FILES · 2 • tests/test_gdpr.py • tests/test_security.py

Art. 30

6741a08a537

PARTIAL HIGH RISK

processor-ropa-documented — Processor records partially documented in `sub-processors.md`. No structured electronic RoPA for processor-side records in Art. 30(2) format.

EVIDENCE FILES · 1 • ee/docs/sub-processors.md

showing · 10 of 32 requirements in this module

Expand all 32

MODULE 02 · 19 REQUIREMENTS

Access Control & Security Measures

18 implemented · 1 partial · 0 gap · 86 active evidence signals

collapsed · 19 requirements

Expand module

MODULE 03 · 16 REQUIREMENTS

International Transfer Governance

0 implemented · 6 partial · 10 gap · 34 active evidence signals

collapsed · 16 requirements

Expand module

§ 05 / 05

PRIORITY GAPS

Priority gaps — sorted by risk.

All 46 gap-status requirements ranked by intrinsic risk: **high-risk** first, then moderate, then low. Use this list to scope the next implementation sprint.

46 Priority Gaps

all gap-status requirements · most-urgent first

sorted by · risk ↓ then module

REQUIREMENT	ARTICLE	MODULE	RISK	DESCRIPTION
e498d504b666	37	Controller Governance & Accountability	High	Implement a DPO qualification assessment and selection process that evaluates candidates against documented criteria including expert knowledge of data protection law.
cddacc002544	37	Controller Governance & Accountability	High	Implement an integrated DPO designation trigger assessment system within the processing activity register that evaluates all three mandatory designation criteria.
f6c2f4858cbe	36	Controller Governance & Accountability	High	Implement an integrated prior consultation management system that: (1) automatically detects when a DPIA residual risk classification remains 'high' even after mitigation review.
9cf8122121f10	35	Controller Governance & Accountability	High	Implement a DPIA review and reassessment process integrated with change management systems, ensuring that processing operations are reviewed against the DPIA whenever changes occur.
5b8c902e534d	49	International Transfer Governance	High	Implement technical controls on public register data export systems to prevent bulk or category-wide exports of personal data to third countries, and require derogation review.
9cc372a77f39	15	International Transfer Governance	High	Maintain a register of all international data transfers to third countries or international organisations, including the applicable Article 46 safeguard.
6649b0b81947	48	International Transfer Governance	High	Implement a formal intake and assessment process for foreign legal orders (court judgments) or administrative decisions from third countries) requiring transfer or disclosure.
c78c59dab8f2	49	International Transfer Governance	High	Implement an integrated third-country transfer governance platform that: (1) manages and logs all derogation-based transfers under Art. 49(1), capturing necessity assessments.
b875a6f6ddc1	45	International Transfer Governance	High	Implement a contingency and incident response capability for adequacy decision revocation events, comprising: (1) a documented contingency plan for each transfer destination.
61caf1e2d8b1	47	International Transfer Governance	High	Implement a monitoring and reporting mechanism to detect and report to the competent supervisory authority any third-country legal requirements (laws, judgments, etc.).

REQUIREMENT	ARTICLE	MODULE	RISK	DESCRIPTION
3c80ae6b6ea8	6	Breach & Change Notification Pipeline	High	Implement a purpose compatibility assessment workflow and register that evaluates and documents whether further processing of personal data for a new purpose is compatible.
211836e9941d1	18	Breach & Change Notification Pipeline	High	Build an automated notification workflow in the data management system that triggers a communication to the data subject before a processing restriction is lifted.
cc4f29f6fcc1	14	Breach & Change Notification Pipeline	High	Implement a purpose-change detection and notification workflow that identifies when personal data obtained indirectly is intended to be processed for a new purpose.
849da1b95698	13	Breach & Change Notification Pipeline	High	Implement a secondary purpose change detection and notification system that identifies when personal data is intended to be processed for a purpose other than originally collected.
0a7502aaf868	14	Breach & Change Notification Pipeline	High	Implement automated workflows that track data acquisition timestamps from third-party sources and enforce delivery of privacy notices within the prescribed window.
cbb9c7ace7d6	14	Breach & Change Notification Pipeline	High	Implement and maintain a comprehensive privacy notice management system for indirect data collection scenarios that: (1) captures and delivers control points.
74cc1fee843c	22	Data Subject Rights Operations	High	Implement a human intervention workflow system with automated decision-making applications that enables data subjects to (a) request human review of automated decisions.
93f85472bb91	26	Data Subject Rights Operations	High	Each joint controller must independently implement operational capability to receive, process, and respond to data subject rights requests (access, erasure, etc.).
a971feeb94c1	21	Data Subject Rights Operations	High	Implement technical mechanisms in information society services to receive, parse, and honour automated objection signals from data subjects (e.g. Global Privacy Control).
5d4cfc7d822c	8	Lawful Basis & Consent Engineering	High	Implement an integrated child consent management system within information society service registration and consent flows that: (1) enforces an age-gate.

showing · 20 of 46 · 26 more · 15 high · 18 moderate · 13 low overall

Show all 46 priority gaps

RuleMesh

RuleMesh turns regulations into structured, citation-backed rules that engineering teams and AI coding agents consume natively. Reports like this are generated on demand from the live audit trail.

REPORT

doc · evidence-signals.gdpr

version · v0.4.2

build · #756a5a7

scope · org_f296b4ca5f78