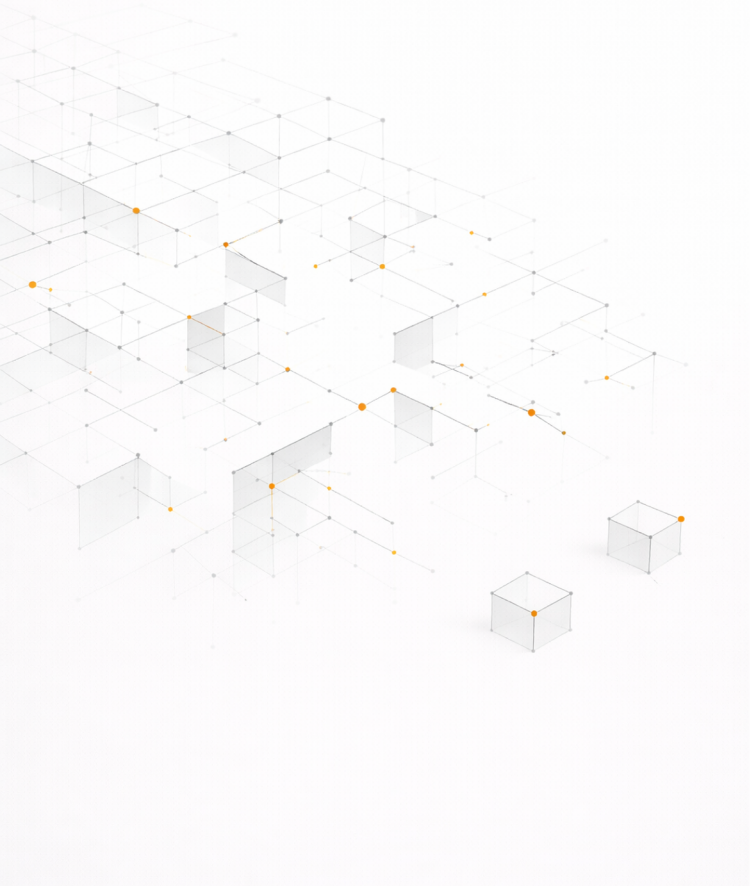

APOLLO Data Auditor

WHITE PAPER · COMPLIANCE

Compliance Is Not a Checkbox

Scoring Your GDPR, CCPA and NIS2 Posture on Real Data

Are Your Data Actually Compliant?

WHY DECLARATIONS ARE NOT PROOF — AND WHAT SCAN-BASED COMPLIANCE CHANGES

Compliance Module — April 2026

EXECUTIVE SUMMARY

€486 million in fines. That is what one European data protection authority alone — the CNIL — imposed in 2025. 42% of those sanctions targeted SMBs.

Most organizations believe they are compliant because they filled out a register, documented their processes, and checked the boxes. But when an authority investigates, it does not ask whether your register is up to date. It asks whether your data matches what your register says. In most cases, it does not.

This paper examines why declaration-based compliance fails, why no existing tool scores compliance at the level regulators actually enforce — by article — and how a scan-based approach closes the gap.

1. THE GAP BETWEEN YOUR REGISTER AND YOUR DATA

A French healthcare software company processed medical data for clinics and hospitals. It had security policies in place. It had documented processes. When the CNIL investigated, it found shared accounts, weak passwords, and inadequate encryption on systems handling health records. The policies existed on paper. The data told a different story. Fine: €1,700,000 for Article 32 violations — insufficient security measures.

The company had declared its data processing activities. But it had never scanned its own systems to verify whether the technical measures matched the declarations.

This is not a French problem. It is a structural one.

In Spain, an identity verification company processed facial biometric data — Article 9 special category data — with pre-checked consent boxes and excessive retention periods. The company had a privacy policy. It had terms of service. What it did not have was a system that flagged "you are processing biometric data without a valid legal basis." The Spanish authority fined them €950,000 — €500,000 for Article 9 alone.

In California, a retail distributor failed to implement proper opt-out mechanisms and did not maintain compliant service provider contracts. This was not a data breach — no attacker was involved. It was a compliance failure discovered during a regulatory audit. The CPPA imposed a record $1,350,000 fine — the largest administrative penalty under CCPA to date.

In France again, the CNIL sanctioned 16 separate organizations in 2025 for covert employee video surveillance — cameras filming workstations continuously, images used for disciplinary purposes without legal basis or employee notification. Each case involved a company that believed its surveillance was lawful because it had a stated purpose. None had verified whether the data collected matched Article 5 principles of proportionality and minimization.

These cases share one pattern: the organization believed it was compliant because it had documentation. The regulator found otherwise because the data told a different story.

The numbers confirm the systemic nature of the problem:

- 42% of CNIL sanctions now target SMBs — up from 15% in 2019. In Spain, 70% of AEPD enforcement actions in 2024 targeted SMBs and sole traders.
- 14 organizations sanctioned by the CNIL in 2025 for Article 32 failures (security). 14 more for DSAR violations (right of access, right of erasure).
- GDPR fines have reached €7.1 billion cumulative across Europe. 443 breach notifications per day — a 22% increase year over year (DLA Piper 2026).
- 20 US states now have comprehensive privacy laws. The CPPA issued its record $1.35M fine in October 2025.
- NIS2 has been transposed in 22 of 27 EU member states. Maximum penalty: €10M or 2% of global revenue. First enforcement actions expected in 2026.

APOLLO IN ACTION — THREE REAL CASES SCORED

Each case above followed the same pattern: documentation existed, but the data contradicted it. Below is what an APOLLO™ Data Auditor scan would have surfaced before the enforcement action.

Case 1 — French Healthcare Software Company, €1,700,000 fine (CNIL 2025)

Scan profile: 3 databases, 12,400 tables. Shared accounts on systems handling health records. Weak password policy. No encryption at rest on storage volumes containing medical data. Article 32 violations confirmed during investigation.

Score	Value	Status
Risk Exposure — S013 Global	**22 / 100**	CRITICAL
Compliance GDPR	9 / 100	Grade F
Data Protection	11 / 100	CRITICAL
Estimated financial exposure	**€ 2,100,000**	—

GDPR Article	Score	Finding
Art. 9 — Sensitive data	0 / 100	Health records in unencrypted tables — 100% unprotected
Art. 32 — Security	0 / 100	Shared accounts detected. No individual credentials. Encryption: 0%.
Art. 30 — Documentation	15 / 100	Register exists but 74% of detected processing activities undeclared
Art. 5 — Retention	45 / 100	Records dating 6+ years, no archiving policy for medical data

Priority	Action	Estimated impact
P1	Eliminate shared accounts — assign individual credentials to all DB users	Art. 32: critical path to compliance
P1	Enable encryption at rest on all volumes storing health data	– €1,100,000 exposure
P1	Update processing register to cover all detected processing activities	Art. 30: from 15 to 70+

The CNIL fine was €1,700,000. APOLLO estimated €2.1M. The register existed — it just didn't reflect reality. A scan would have flagged the 74% gap between declared and detected processing before the investigation opened.

Case 2 — Spanish Identity Verification Company, €950,000 fine (AEPD 2024)

Scan profile: 1 database, 890,000 records. Data types: facial biometric images, identity document scans — Article 9 special category. Consent collected via pre-checked opt-in boxes. Retention: biometric data kept indefinitely with no deletion schedule.

Score	Value	Status
Risk Exposure — S013 Global	**14 / 100**	CRITICAL
Compliance GDPR	4 / 100	Grade F
Data Protection	18 / 100	CRITICAL
Estimated financial exposure	**€ 1,200,000**	—

GDPR Article	Score	Finding
Art. 9 — Sensitive data	0 / 100	Biometric data + identity documents = maximum sensitivity. No valid legal basis.
Art. 32 — Security	12 / 100	Encryption present but no access control on biometric table
Art. 30 — Documentation	20 / 100	Processing activity declared, legal basis not validated
Art. 5 — Retention	0 / 100	Zero deletion policy. Biometric data retained indefinitely.

Priority	Action	Estimated impact
P1	Define and enforce retention limit for biometric data (12-month maximum)	Art. 5: from 0 to compliant
P1	Replace pre-checked consent with explicit opt-in — rebuild legal basis	Art. 9: required before any further processing
P2	Restrict biometric table access to 3 named accounts (current: open)	Art. 32: from 12 to partial compliance

The AEPD fine was €950,000 — €500,000 for Art. 9 alone. APOLLO estimated €1.2M. The company had a privacy policy. What it did not have was a system that flagged "you are retaining biometric data with no deletion schedule and no verified legal basis." APOLLO flags that on scan day one.

Case 3 — California Retail Distributor, $1,350,000 fine (CPPA 2025)

Scan profile: CRM database, 2.3M consumer records. No opt-out mechanism detected in data flows. Service provider contracts missing data processing clauses. No consent record for third-party data sharing. CCPA compliance assessed: non-functional.

Score	Value	Status
Risk Exposure — S013 Global	**31 / 100**	CRITICAL
Compliance CCPA	Grade F	CRITICAL
Data Protection	38 / 100	CRITICAL
Estimated financial exposure	**$1,650,000**	—

CCPA Requirement	Score	Finding
Right to opt-out	0 / 100	No opt-out mechanism detected in data flows
Service provider contracts	0 / 100	0 of 7 vendors have compliant data processing addendums
Consent records	15 / 100	Third-party sharing active, consent basis undocumented
Data subject rights	40 / 100	DSAR process exists but not tested against live data

Priority	Action	Estimated impact
P1	Implement opt-out mechanism across all consumer touchpoints	CCPA: removes primary violation category
P1	Execute data processing addendums with all 7 active vendors	Required — currently 0 compliant contracts
P2	Map all third-party data flows against consent records	Closes consent gap for 2.3M records

The CPPA fine was $1,350,000 — the largest administrative penalty under CCPA to date. This was not a breach. No attacker was involved. It was a compliance audit on live data. APOLLO scans the actual data flows, not the declared ones — which is exactly what the regulator did.

2. WHY EXISTING TOOLS DON'T SCORE WHAT REGULATORS ENFORCE

When a European data protection authority investigates, it does not ask "what is your overall compliance maturity score?" It asks specific questions tied to specific articles: Did you identify all special category data under Article 9? Are your technical security measures proportionate under Article 32? Is your processing register complete under Article 30?

No existing tool — at any price point — answers these questions with a grade based on actual data.

What regulators enforce	GRC / Compliance automation	Privacy governance (DPO tools)	Enterprise DSPM platforms	APOLLO
GDPR Art. 9 — Special category data	❌ Checklist: "Do you process health data?"	❌ Declarative DPIA	⚠️ Can detect, doesn't grade by article	✅ **Score A-F: detects Art.9 PII in your files, grades compliance**
GDPR Art. 30 — Processing register	⚠️ Template you fill manually	✅ Workflow, but declarative	❌ Not their scope	✅ **Score A-F: compares declared vs detected processing activities**
GDPR Art. 32 — Security measures	⚠️ Verifies controls exist	❌ Not technical	⚠️ Evaluates posture, not per-article	✅ **Score A-F: encryption, access control, backup — measured, not declared**
CCPA — Consumer data mapping	⚠️ Templates	❌ Not covered	⚠️ Data discovery, no CCPA scoring	✅ **Gap analysis with penalty calculation**
NIS2 — Cybersecurity posture	❌ Not covered	❌ Not covered	⚠️ Partial	✅ **Gap analysis**
SOC2 — 5 TSC pillars	✅ Native (their core market)	❌ Not covered	❌ Not their scope	✅ **Gap analysis**
DORA — Digital resilience	❌ Not covered	❌ Not covered	❌ Not covered	✅ **Gap analysis**
Method	Declarations + cloud monitoring	Questionnaires	Data scan (no per-article scoring)	**Data scan + per-article scoring**
Price	$10K–$200K/yr	€5K–€50K/yr	$50K–$500K/yr	**< €5K/yr**

The critical gap: on 14 competitors verified in April 2026 — including enterprise DSPM platforms at $250K+/year — none produces a GDPR compliance score by article (Art. 5, 9, 30, 32) with A-F grades based on a real data scan. Not one.

GRC platforms excel at SOC2 and ISO 27001 — frameworks built around documented controls. But GDPR is enforced by article, against actual data. A SOC2 certification does not tell you that 340 files in your HR directory contain unencrypted health data in violation of Article 9.

To cover GDPR + CCPA + NIS2 + SOC2 + DORA, an SMB would need to combine three to five tools and consultants — at a combined cost exceeding €50K/year. That is not realistic.

---

3. WHAT SCAN-BASED COMPLIANCE ACTUALLY MEANS

A DPO preparing for a regulatory audit has two options today.

Option A — declarative. Open the processing register (Article 30). Review each declared processing activity. Cross-reference with the privacy impact assessments. Ask department heads whether anything has changed. Hope that what people declared still reflects reality. Time: 2–4 weeks. Cost: €5K–€15K if outsourced. Confidence: low — because the register is only as good as the last person who updated it.

Option B — scan-based. Run an automated scan across all data sources — files, databases, cloud storage, Active Directory. The scan detects every PII type present, maps where it lives, identifies what articles apply, and grades compliance for each article against the actual data found. Time: 48 hours. Output: a score per article (A through F), a prioritized remediation plan (P1/P2/P3), and a financial estimate of what non-compliance costs.

The difference is the difference between asking "are we compliant?" and proving it.

What scan-based compliance produces:

Article-level scoring. Not "your GDPR maturity is 67%." Instead: "Your Article 32 is D — 340 files with health data are unencrypted. Your Article 9 is F — biometric data detected in 3 databases without a DPIA. Your Article 30 is B — 2 undeclared processing activities identified." Each score comes with the specific findings that drive it.

Multi-framework coverage in a single scan. GDPR by article, CCPA gap analysis, NIS2 cybersecurity posture, SOC2 readiness across 5 Trust Service Criteria, DORA digital resilience assessment. Five frameworks, one scan, one dashboard. Not five questionnaires from five vendors.

A remediation plan tied to financial impact. Each corrective action (P1/P2/P3) shows what it fixes, which article it addresses, and what the penalty reduction would be if implemented. A DPO can prioritize by regulatory risk, not by gut feeling.

What-if analysis. Select a corrective action and see the exact recalculation of your GDPR/CCPA penalty exposure. "If we encrypt these 340 health files, Article 32 moves from D to B, and exposure drops by €180K." This turns compliance from a checkbox exercise into a financial optimization.

---

4. HOW APOLLO DATA AUDITOR SCORES COMPLIANCE

The capabilities described above exist today. Here is how they work in practice.

Your data stays yours. A native agent runs locally on your infrastructure — Windows, Linux, and macOS (arm64). It scans 11 source types: files, PostgreSQL, MySQL, MongoDB, SQL Server, OneDrive, SharePoint, Active Directory/LDAP, ERP, NFS/SMB, and infrastructure. Only metadata and counters transit to the cloud dashboard. Raw data never leaves your perimeter. The agent is open source (BSL 1.1) — verifiable on GitHub.

You get a compliance score by article — not by framework. The dashboard breaks down GDPR into individual articles (Art. 5, 9, 30, 32), each graded A through F based on the PII detected, the security measures in place, and the processing activities identified. CCPA gets its own scoring panel with gap analysis. NIS2 and SOC2 get readiness assessments. DORA gets a digital resilience score.

US multi-state privacy coverage. Beyond CCPA, the dashboard includes a 50-state privacy landscape — revenue-based thresholds, cure periods, and enforcement mechanisms for each state. 20 states now have comprehensive privacy laws. Your compliance exposure is not just California.

You get a remediation plan that calculates itself. Priority actions (P1/P2/P3) are tied to specific articles, specific findings, and specific financial impacts. The What-If engine recalculates your penalty exposure in real time as you select corrective actions. The DPO sees exactly what each fix is worth in euros or dollars.

Every score is transparent, reproducible, and published. No black box.

THE PRICE COMPARISON

	GRC platforms (SOC2-first)	Privacy tools (DPO)	Enterprise DSPM	APOLLO Data Auditor
Annual cost	$10,000 – $200,000	€5,000 – €50,000	$50,000 – $500,000	**€2,999 / year** (Starter)
GDPR by article (A–F)	No	No	No	**Yes**
Frameworks covered	2–3 (SOC2 focus)	1 (GDPR only)	3–5 (partial)	**5 (GDPR, CCPA, NIS2, SOC2, DORA)**
Method	Declarations	Questionnaires	Scan (no per-article)	**Scan + per-article scoring**
Remediation with €/$ impact	Generic	Generic	Partial	**Yes — per action**

5. ONE SCAN. ONE ANSWER. FOUR DIMENSIONS.

Compliance is not an isolated problem. An Article 9 violation is also a financial exposure. A missing encryption control is both a compliance gap and a data protection risk. An unaudited database is a compliance blind spot and an AI readiness blocker.

Most organizations treat these as separate workstreams — separate tools, separate budgets, separate timelines. APOLLO was built on the premise that they are one problem, measured in one scan.

→ **Compliance** — what this paper covers. GDPR scored by article (A-F), CCPA, NIS2, SOC2, DORA. Based on actual data, not declarations. Remediation plan with financial impact per action.

→ **Risk Exposure** — financial quantification in € and $, breach impact simulation, PII mapping, toxic combinations, risk zones.

→ **Data Protection** — encryption coverage, backup resilience, ransomware readiness simulation, access control hygiene, dormant account detection.

→ **Intelligence** — AI Readiness scoring, data quality metrics, AI Act pre-compliance (Article 10 data governance, Article 15 cybersecurity posture).

No other tool under €5,000/year covers all four. The reason is structural: enterprise platforms were built for Fortune 500 procurement cycles. GRC tools were built around SOC2 checkboxes. Privacy tools were built for DPO workflows. None were built to

answer the question an SMB actually needs answered: what is the real state of my data, across all the regulations that apply to me, and what do I do first?

APOLLO™ Data Auditor exists because the answer should not require a €100K budget.

Sources: CNIL Bilan sanctions 2025 · DLA Piper GDPR Fines & Data Breach Survey 2026 · CMS GDPR Enforcement Tracker 2024/2025 · CPPA CCPA Fines 2025 · AEPD FY24 via Linklaters TechInsights · ECSO NIS2 Transposition Tracker · IBM Cost of a Data Breach Report 2024 & 2025 · Forrester/Cyera Data Security Study 2024 · DataGuidance AEPD enforcement · Enforcement Tracker (enforcementtracker.com)

APOLLO™ Data Auditor Every file is a risk. Measure it.

→ https://apollo.aiia-tech.com → GitHub: https://ggabrie2025.github.io/apollo_data_auditor/ → contact@aiia-tech.com