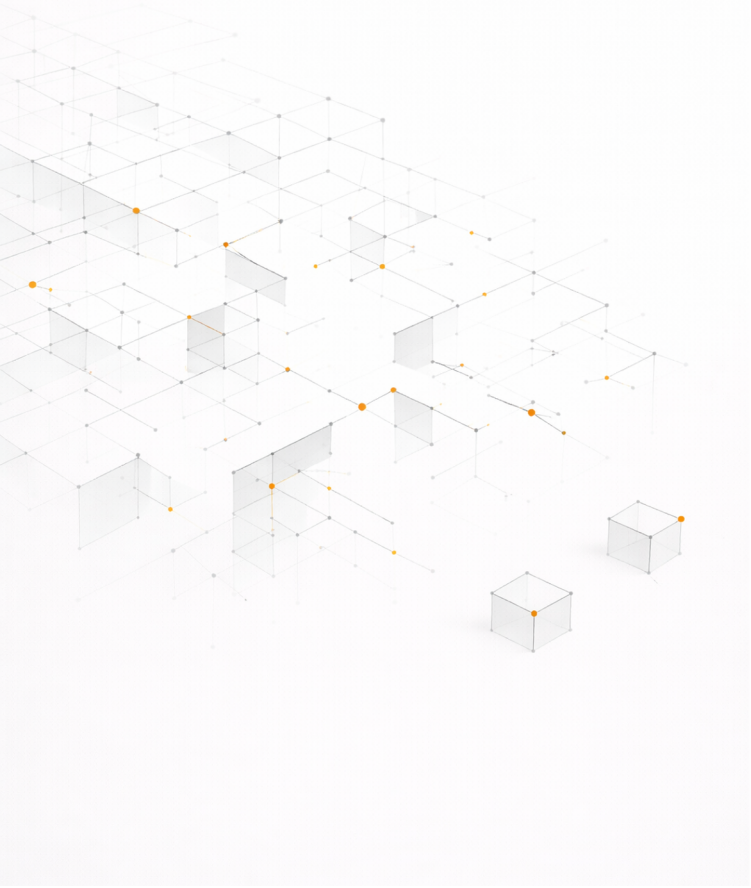

APOLLO Data Auditor

LIVRE BLANC · CONFORMITÉ

La conformité n'est pas une case à cocher

Scorer votre posture RGPD, CCPA et NIS2 sur données réelles

Vos données sont-elles vraiment conformes ?

POURQUOI LES DÉCLARATIONS NE SONT PAS LA PREUVE — ET COMMENT LA CONFORMITÉ BASÉE SUR LES SCANS CHANGE LES CHOSES

Module Compliance — Avril 2026

RÉSUMÉ EXÉCUTIF

486 millions d'euros d'amendes. C'est ce que seule une autorité européenne de protection des données — la CNIL — a imposé en 2025. 42% de ces sanctions visaient des PME.

La plupart des organisations croient être conformes parce qu'elles ont rempli un registre, documenté leurs processus et coché les cases. Mais lorsqu'une autorité enquête, elle ne demande pas si votre registre est à jour. Elle demande si vos données correspondent à ce que votre registre dit. Dans la plupart des cas, ce n'est pas le cas.

Ce document examine pourquoi la conformité basée sur les déclarations échoue, pourquoi aucun outil existant ne note la conformité au niveau que les régulateurs appliquent réellement — par article — et comment une approche basée sur les scans comble le fossé.

1. LE FOSSÉ ENTRE VOTRE REGISTRE ET VOS DONNÉES

Une entreprise française de logiciels de santé traitait des données médicales pour des cliniques et des hôpitaux. Elle avait des politiques de sécurité en place. Elle avait documenté ses processus. Lorsque la CNIL a enquêté, elle a découvert des comptes partagés, des mots de passe faibles et un chiffrement inadéquat sur les systèmes traitant les dossiers médicaux. Les politiques existaient sur papier. Les données racontaient une histoire différente. Amende : 1 700 000 € pour violations de l'article 32 — mesures de sécurité insuffisantes.

L'entreprise avait déclaré ses activités de traitement de données. Mais elle n'avait jamais analysé ses propres systèmes pour vérifier si les mesures techniques correspondaient aux déclarations.

Ce n'est pas un problème français. C'est un problème structurel.

En Espagne, une entreprise de vérification d'identité traitait des données de reconnaissance faciale — données de catégorie spéciale de l'article 9 — avec des cases de consentement précochées et des périodes de conservation excessives. L'entreprise avait une politique de confidentialité. Elle avait des conditions de service. Ce qu'elle n'avait pas, c'était un système qui signalait « vous traitez des données biométriques sans base légale valide ». L'autorité espagnole les a condamnés à une amende de 950 000 € — 500 000 € pour l'article 9 seul.

En Californie, un distributeur de détail n'a pas mis en œuvre de mécanismes de désinscription appropriés et n'a pas maintenu de contrats de prestataires de services conformes. Ce n'était pas une brèche de données — aucun attaquant n'était impliqué. C'était un défaut de conformité découvert lors d'un audit réglementaire. Le CPPA a imposé une amende record de 1 350 000 $ — la plus grande pénalité administrative en vertu de la CCPA à ce jour.

En France à nouveau, la CNIL a sanctionné 16 organisations distinctes en 2025 pour surveillance vidéo secrète d'employés — des caméras filmant continuellement les postes de travail, les images utilisées à des fins disciplinaires sans base légale ou notification aux employés. Chaque cas impliquait une entreprise qui croyait que sa surveillance était légale parce qu'elle avait un but déclaré. Aucune n'avait vérifié si les données collectées correspondaient aux principes de proportionnalité et de minimisation de l'article 5.

Ces cas partagent un motif : l'organisation croyait être conforme parce qu'elle avait une documentation. Le régulateur a constaté le contraire parce que les données racontaient une histoire différente.

Les chiffres confirment la nature systémique du problème :

- 42% des sanctions de la CNIL ciblent maintenant les PME — contre 15% en 2019. En Espagne, 70% des actions d'exécution de l'AEPD en 2024 visaient les PME et les travailleurs indépendants.
- 14 organisations sanctionnées par la CNIL en 2025 pour défaillances de l'article 32 (sécurité). 14 autres pour violations de DSAR (droit d'accès, droit à l'oubli).

- Les amendes RGPD ont atteint 7,1 milliards d'€ cumulés en Europe. 443 notifications de brèche par jour — une augmentation de 22% d'année en année (DLA Piper 2026).
- 20 États américains disposent maintenant de lois complètes sur la confidentialité. Le CPPA a imposé son amende record de 1,35 M$ en octobre 2025.
- NIS2 a été transposée dans 22 des 27 États membres de l'UE. Pénalité maximale : 10 M€ ou 2% du chiffre d'affaires mondial. Les premières actions d'exécution sont attendues en 2026.

APOLLO™ DATA AUDITOR EN ACTION — TROIS CAS RÉELS SCORÉS

Chacun des cas ci-dessus suit le même schéma : la documentation existait, mais les données la contredisaient. Voici ce qu'un scan APOLLO™ Data Auditor aurait détecté avant l'action d'exécution réglementaire.

Cas 1 — Société française de logiciels de santé, amende de 1 700 000 € (CNIL 2025)

Profil de scan : 3 bases de données, 12 400 tables. Comptes partagés sur les systèmes traitant des données de santé. Politique de mots de passe faible. Pas de chiffrement au repos sur les volumes de stockage contenant des données médicales. Violations de l'article 32 confirmées lors de l'enquête.

Score	Valeur	Statut
Exposition au Risque — S013 Global	**22 / 100**	CRITIQUE
Conformité RGPD	9 / 100	Note F
Protection des Données	11 / 100	CRITIQUE
Exposition financière estimée	**2 100 000 €**	—

Article RGPD	Score	Constat
Art. 9 — Données sensibles	0 / 100	Données de santé dans des tables non chiffrées — 100% non protégées
Art. 32 — Sécurité	0 / 100	Comptes partagés détectés. Pas d'identifiants individuels. Chiffrement : 0%.
Art. 30 — Documentation	15 / 100	Registre existant mais 74% des activités de traitement détectées non déclarées
Art. 5 — Conservation	45 / 100	Enregistrements datant de plus de 6 ans, pas de politique d'archivage pour les données médicales

Priorité	Action	Impact estimé
P1	Éliminer les comptes partagés — attribuer des identifiants individuels à tous les utilisateurs DB	Art. 32 : chemin critique vers la conformité
P1	Activer le chiffrement au repos sur tous les volumes stockant des données de santé	– 1 100 000 € d'exposition
P1	Mettre à jour le registre pour couvrir toutes les activités de traitement détectées	Art. 30 : de 15 à 70+

L'amende CNIL était de 1 700 000 €. APOLLO estimait 2,1 M€. Le registre existait — il ne reflétait tout simplement pas la réalité. Un scan aurait signalé l'écart de 74% entre traitements déclarés et détectés avant l'ouverture de l'enquête.

Cas 2 — Société espagnole de vérification d'identité, amende de 950 000 € (AEPD 2024)

Profil de scan : 1 base de données, 890 000 enregistrements. Types de données : images biométriques faciales, scans de documents d'identité — catégorie spéciale article 9. Consentement recueilli via des cases pré-cochées. Conservation : données biométriques conservées indéfiniment sans calendrier de suppression.

Score	Valeur	Statut
Exposition au Risque — S013 Global	**14 / 100**	CRITIQUE
Conformité RGPD	4 / 100	Note F
Protection des Données	18 / 100	CRITIQUE
Exposition financière estimée	**1 200 000 €**	—

Article RGPD	Score	Constat
Art. 9 — Données sensibles	0 / 100	Données biométriques + documents d'identité = sensibilité maximale. Pas de base légale valide.
Art. 32 — Sécurité	12 / 100	Chiffrement présent mais pas de contrôle d'accès sur la table biométrique
Art. 30 — Documentation	20 / 100	Activité de traitement déclarée, base légale non validée
Art. 5 — Conservation	0 / 100	Zéro politique de suppression. Données biométriques conservées indéfiniment.

Priorité	Action	Impact estimé
P1	Définir et appliquer une limite de conservation pour les données biométriques (12 mois maximum)	Art. 5 : de 0 à conforme
P1	Remplacer le consentement pré-coché par un opt-in explicite — reconstruire la base légale	Art. 9 : requis avant tout traitement ultérieur
P2	Restreindre l'accès à la table biométrique à 3 comptes nommés (actuel : ouvert)	Art. 32 : de 12 à conformité partielle

L'amende AEPD était de 950 000 € — 500 000 € pour l'Art. 9 seul. APOLLO estimait 1,2 M€. La société avait une politique de confidentialité. Ce qu'elle n'avait pas, c'est un système signalant « vous conservez des données biométriques sans calendrier de suppression et sans base légale vérifiée ». APOLLO signale cela dès le premier jour du scan.

Cas 3 — Distributeur de détail californien, amende de 1 350 000 $ (CPPA 2025)

Profil de scan : base de données CRM, 2,3 millions d'enregistrements consommateurs. Pas de mécanisme d'opt-out détecté dans les flux de données. Contrats prestataires manquant de clauses de traitement des données. Pas d'enregistrement de consentement pour le partage avec des tiers. Conformité CCPA évaluée : non fonctionnelle.

Score	Valeur	Statut
Exposition au Risque — S013 Global	**31 / 100**	CRITIQUE
Conformité CCPA	Note F	CRITIQUE
Protection des Données	38 / 100	CRITIQUE
Exposition financière estimée	**1 650 000 $**	—

Exigence CCPA	Score	Constat
Droit d'opt-out	0 / 100	Pas de mécanisme d'opt-out détecté dans les flux de données
Contrats prestataires	0 / 100	0 sur 7 prestataires ont des avenants de traitement des données conformes
Enregistrements de consentement	15 / 100	Partage avec des tiers actif, base de consentement non documentée
Droits des personnes concernées	40 / 100	Processus DSAR existant mais non testé sur données réelles

Priorité	Action	Impact estimé
P1	Implémenter un mécanisme d'opt-out sur tous les points de contact consommateurs	CCPA : supprime la catégorie de violation principale
P1	Exécuter des avenants de traitement des données avec les 7 prestataires actifs	Requis — actuellement 0 contrat conforme
P2	Cartographier tous les flux de données tiers par rapport aux enregistrements de consentement	Ferme l'écart de consentement pour 2,3 M d'enregistrements

L'amende CPPA était de 1 350 000 $ — la sanction administrative la plus élevée jamais prononcée sous CCPA. Il ne s'agissait pas d'une brèche. Aucun attaquant n'était impliqué. C'était un audit de conformité sur des données réelles. APOLLO analyse les flux de données réels, pas les déclarés — exactement ce qu'a fait le régulateur.

---

2. POURQUOI LES OUTILS EXISTANTS NE NOTENT PAS CE QUE LES RÉGULATEURS APPLIQUENT

Lorsqu'une autorité européenne de protection des données enquête, elle ne demande pas « quel est votre score global de maturité de conformité ? » Elle pose des questions spécifiques liées aux articles spécifiques : Avez-vous identifié tous les données de catégorie spéciale en vertu de l'article 9 ? Vos mesures de sécurité technique sont-elles proportionnées en vertu de l'article 32 ? Votre registre des traitements est-il complet en vertu de l'article 30 ?

Aucun outil existant — à aucun prix — ne répond à ces questions avec une note basée sur les données réelles.

Ce que les régulateurs appliquent	Automatisation GRC / Conformité	Gouvernance de la vie privée (outils DPD)	Plateformes DSPM d'entreprise	APOLLO
RGPD Art. 9 — Données de catégorie spéciale	❌ Checklist : « Traitez-vous des données de santé ? »	❌ DPIA déclarative	⚠️ Peut détecter, ne note pas par article	✅ **Note A-F : détecte les données d'identité de l'art.9 dans vos fichiers, note la conformité**
RGPD Art. 30 — Registre des traitements	⚠️ Modèle que vous remplissez manuellement	✅ Flux de travail, mais déclaratif	❌ Pas de leur ressort	✅ **Note A-F : compare les activités de traitement déclarées vs détectées**
RGPD Art. 32 — Mesures de sécurité	⚠️ Vérifie l'existence des contrôles	❌ Pas technique	⚠️ Évalue la posture, pas par article	✅ **Note A-F : chiffrement, contrôle d'accès, sauvegarde — mesurés, pas déclarés**
CCPA — Cartographie des données du consommateur	⚠️ Modèles	❌ Non couverts	⚠️ Découverte de données, pas de notation CCPA	✅ **Analyse des lacunes avec calcul de pénalité**
NIS2 — Posture cybersécurité	❌ Non couverts	❌ Non couverts	⚠️ Partiel	✅ **Analyse des lacunes**
SOC2 — 5 piliers TSC	✅ Natif (leur marché principal)	❌ Non couverts	❌ Pas de leur ressort	✅ **Analyse des lacunes**
DORA — Résilience numérique	❌ Non couverts	❌ Non couverts	❌ Non couverts	✅ **Analyse des lacunes**
Méthode	Déclarations + surveillance cloud	Questionnaires	Scan de données (pas de notation par article)	**Scan de données + notation par article**
Prix	10 000 $ – 200 000 $/an	5 000 € – 50 000 €/an	50 000 $ – 500 000 $/an	**< 5 000 €/an**

Le fossé critique : sur 14 concurrents vérifiés en avril 2026 — y compris les plateformes DSPM d'entreprise à 250 000 €+/an — aucun ne produit de note de conformité RGPD par article (Art. 5, 9, 30, 32) avec des notes A-F basées sur un vrai scan de données. Pas un seul.

Les plateformes GRC excellent en SOC2 et ISO 27001 — des frameworks construit autour de contrôles documentés. Mais le RGPD est appliqué par article, contre les données réelles. Une certification SOC2 ne vous dit pas que 340 fichiers dans votre répertoire RH contiennent des données de santé non chiffrées en violation de l'article 9.

Pour couvrir RGPD + CCPA + NIS2 + SOC2 + DORA, une PME aurait besoin de combiner trois à cinq outils et consultants — à un coût combiné dépassant 50 000 €/an. Ce n'est pas réaliste.

---

3. CE QUE LA CONFORMITÉ BASÉE SUR LES SCANS SIGNIFIE RÉELLEMENT

Un DPD préparant un audit réglementaire a deux options aujourd'hui.

Option A — déclarative. Ouvrir le registre des traitements (article 30). Examiner chaque activité de traitement déclarée. Croiser les références avec les études d'impact relatives à la vie privée. Demander aux chefs de département si quelque chose a changé. Espérer que ce que les gens ont déclaré reflète toujours la réalité. Temps : 2–4 semaines. Coût : 5 000 € – 15 000 € si externalisé. Confiance : faible — parce que le registre n'est aussi bon que la dernière personne qui l'a mis à jour.

Option B — basée sur les scans. Lancer un scan automatisé sur toutes les sources de données — fichiers, bases de données, stockage cloud, Active Directory. Le scan détecte chaque type de données d'identité présent, cartographie où il réside, identifie quels articles s'appliquent et note la conformité pour chaque article par rapport aux données réelles trouvées. Temps : 48 heures. Résultat : une note par article (A à F), un plan de remédiation priorisé (P1/P2/P3) et une estimation financière de ce que le non-respect coûte.

La différence est la différence entre demander « sommes-nous conformes ? » et le prouver.

Ce que la conformité basée sur les scans produit :

Notation au niveau de l'article. Pas « votre maturité RGPD est de 67% ». Au lieu de cela : « Votre article 32 est D — 340 fichiers contenant des données de santé ne sont pas chiffrés. Votre article 9 est F — données biométriques détectées dans 3 bases de données sans DPIA valide. Votre article 30 est B — 2 activités de traitement non

déclarées identifiées. » Chaque note s'accompagne des conclusions spécifiques qui la motivent.

Couverture multi-framework en un seul scan. RGPD par article, analyse des lacunes CCPA, posture cybersécurité NIS2, préparation SOC2 sur 5 critères de service de confiance, évaluation de résilience numérique DORA. Cinq frameworks, un scan, un tableau de bord. Pas cinq questionnaires de cinq fournisseurs.

Un plan de remédiation lié à l'impact financier. Chaque action corrective (P1/P2/P3) montre ce qu'elle corrige, quel article elle aborde et quelle serait la réduction de pénalité en cas de mise en œuvre. Un DPD peut prioriser par risque réglementaire, pas par intuition.

Analyse de scénarios. Sélectionnez une action corrective et voyez le recalcul exact de votre exposition aux pénalités RGPD/CCPA. « Si nous chiffrons ces 340 fichiers de santé, l'article 32 passe de D à B, et l'exposition baisse de 180 000 € ». Cela transforme la conformité d'un exercice de case à cocher en optimisation financière.

---

4. COMMENT APOLLO DATA AUDITOR NOTE LA CONFORMITÉ

Les capacités décrites ci-dessus existent aujourd'hui. Voici comment elles fonctionnent en pratique.

Vos données restent les vôtres. Un agent natif s'exécute localement sur votre infrastructure — Windows, Linux et macOS (arm64). Il analyse 11 types de sources : fichiers, PostgreSQL, MySQL, MongoDB, SQL Server, OneDrive, SharePoint, Active Directory/LDAP, ERP, NFS/SMB et infrastructure. Seules les métadonnées et les compteurs transitent vers le tableau de bord cloud. Les données brutes ne quittent jamais votre périmètre. L'agent est open source (BSL 1.1) — vérifiable sur GitHub.

Vous obtenez une note de conformité par article — pas par framework. Le tableau de bord décompose le RGPD en articles individuels (Art. 5, 9, 30, 32), chacun noté de A à F en fonction des données d'identité détectées, des mesures de sécurité en place et des activités de traitement identifiées. La CCPA reçoit son propre panneau de notation avec analyse des lacunes. NIS2 et SOC2 reçoivent des évaluations de préparation. DORA reçoit une note de résilience numérique.

Couverture de la vie privée multi-États américains. Au-delà de la CCPA, le tableau de bord inclut un paysage de vie privée sur 50 États — seuils basés sur les revenus, périodes de remédiation et mécanismes d'exécution pour chaque État. 20 États disposent maintenant de lois complètes sur la vie privée. Votre exposition à la conformité ne concerne pas seulement la Californie.

Vous obtenez un plan de remédiation qui se calcule de lui-même. Les actions prioritaires (P1/P2/P3) sont liées aux articles spécifiques, aux conclusions spécifiques et aux impacts financiers spécifiques. Le moteur What-If recalcule votre exposition aux pénalités en temps réel au fur et à mesure que vous sélectionnez des actions correctives. Le DPD voit exactement ce que chaque correction vaut en euros ou en dollars.

Chaque note est transparente, reproductible et publiée. Pas de boîte noire.

LA COMPARAISON DES PRIX

	Plateformes GRC (orientation SOC2)	Outils de vie privée (DPD)	DSPM d'entreprise	APOLLO Data Auditor
Coût annuel	10 000 $ - 200 000 $	5 000 € - 50 000 €	50 000 $ - 500 000 $	**2 999 € / an** (Starter)
RGPD par article (A-F)	Non	Non	Non	**Oui**
Frameworks couverts	2-3 (orientation SOC2)	1 (RGPD uniquement)	3-5 (partiel)	**5 (RGPD, CCPA, NIS2, SOC2, DORA)**
Méthode	Déclarations	Questionnaires	Scan (pas de notation par article)	**Scan + notation par article**
Remédiation avec impact €/$	Générique	Générique	Partiel	**Oui — par action**

5. UN SCAN. UNE RÉPONSE. QUATRE DIMENSIONS.

La conformité n'est pas un problème isolé. Une violation de l'article 9 est aussi une exposition financière. Un contrôle de chiffrement manquant est à la fois une lacune de

conformité et un risque de protection des données. Une base de données non auditée est une lacune de conformité et un bloqueur de préparation à l'IA.

La plupart des organisations traitent ces éléments comme des flux de travail séparés — outils séparés, budgets séparés, calendriers séparés. APOLLO a été construit sur la prémisse qu'ils constituent un seul problème, mesuré en un seul scan.

→ **Compliance** — ce que ce document couvre. RGPD noté par article (A-F), CCPA, NIS2, SOC2, DORA. Basé sur les données réelles, pas les déclarations. Plan de remédiation avec impact financier par action.

→ **Risk Exposure** — quantification financière en € et $, simulation d'impact de brèche, cartographie des données d'identité, combinaisons toxiques, zones à risque.

→ **Data Protection** — couverture de chiffrement, résilience des sauvegardes, simulation de préparation aux ransomwares, hygiène du contrôle d'accès, détection des comptes dormants.

→ **Intelligence** — Score de préparation à l'IA, métriques de qualité des données, pré-conformité à la loi sur l'IA (gouvernance des données article 10, posture cybersécurité article 15).

Aucun autre outil sous 5 000 €/an ne couvre tous les quatre. La raison en est structurelle : les plateformes d'entreprise ont été construites pour les cycles d'approvisionnement Fortune 500. Les outils GRC ont été construits autour des cases à cocher SOC2. Les outils de vie privée ont été construits pour les flux de travail DPD. Aucun n'a été construit pour répondre à la question qu'une PME doit réellement poser : quel est l'état réel de mes données, parmi toutes les réglementations qui s'appliquent à moi, et par quoi je commence ?

APOLLO™ Data Auditor existe parce que la réponse ne devrait pas nécessiter un budget de 100 000 €.

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 Tout fichier est un risque. Mesurez-le.

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