Macif Vie : la politique écrite, preuve de la négligence

Le 12 novembre 2026, la formation restreinte de la CNIL a infligé 5 millions d'euros d'amende à un assureur-vie que la presse identifie comme Macif Vie, pour des mots de passe conservés en clair et des données gardées trop longtemps, sans qu'aucune fuite soit établie. La couverture y a vu une erreur de débutant. La délibération décrit une organisation qui avait écrit la règle, et c'est l'écart entre cette règle et ses bases de données qui a servi à qualifier sa négligence. Chris Argyris et Donald Schön ont nommé cet écart en 1974 : la distance entre la théorie professée (ce qu'une organisation déclare faire) et la théorie d'usage (ce qui gouverne effectivement ses pratiques).

Par Alexandre Berge · 26 novembre 2026 · 12 min de lecture · Actualité

Cinq millions d'euros sans fuite, à la date du 23 novembre 2026

Alertée le 27 décembre 2023, la CNIL contrôle l'assureur sur place le 14 mai 2024. Elle y trouve près de 1,8 million de mots de passe d'accès aux espaces clients stockés sans aucune fonction de hachage (la transformation d'un mot de passe en empreinte non réversible), dont 730 289 figurent aussi en clair dans une table de journalisation (le registre technique des tentatives de connexion). Huit salariés se partagent l'accès à la base des 1,3 million de clients ayant un contrat en cours, ainsi que le mot de passe administrateur de l'outil qui en affiche les tables.

La délibération SAN-2026-016, adoptée le 12 novembre 2026 et publiée le 18, retient deux manquements au RGPD : l'article 32 (sécurité des traitements) et l'article 5-1-e (limitation de la durée de conservation). Elle désigne l'entreprise comme « société X ». Next l'identifie comme Macif Vie en s'appuyant sur le compte rendu de la séance du 15 octobre publié par l'agence Mlex, et Silicon.fr rapporte que la Macif a confirmé être concernée.

Le récit s'est construit autour de l'évidence. Next y lit « une illustration flagrante de ce qu'il ne faut pas faire », et la délibération rappelle elle-même que l'ANSSI recommande depuis 2013 de hacher et saler les mots de passe. L'affaire a été racontée comme une faute élémentaire. La chronique « Macif Vie : l'écart toléré, jugé avant l'incident », publiée ici le 25 octobre, laissait une question ouverte. La formation restreinte suivrait-elle le rapporteur jusqu'à sanctionner un état du système, en l'absence de tout incident ?

La délibération sanctionne l'état du système et motive peu son montant

La réponse figure au paragraphe 35. À la société qui invoquait l'absence d'incident, la formation restreinte oppose qu'en stockant les mots de passe en clair, elle a rendu vulnérables toutes les données des espaces clients, « peu important que cette vulnérabilité ait été exploitée ou non par un attaquant ».

Le montant appelle plus de prudence. Le rapporteur proposait d'abord 9 millions d'euros, calculés sur le chiffre d'affaires du groupe, puis 7 millions après avoir pris acte de l'absence de données de santé. La formation restreinte confirme l'assiette du groupe, en vertu d'un arrêt de la Cour de justice de l'Union européenne du 5 décembre 2023 qui impose de raisonner sur l'unité économique (l'ensemble des sociétés sous influence dominante commune). Elle fixe l'amende à 5 millions d'euros, montant qui lui « apparait adapté », sans motiver spécifiquement l'écart avec la dernière proposition. Le communiqué cite la gravité des manquements, le nombre de personnes concernées et les capacités financières de la société.

L'injonction sous astreinte devient sans objet, et la publication nominative demandée par le rapporteur est écartée. **Le principe de la sanction sans incident est confirmé. Mais ce qui pèse dans la qualification de la faute n'est pas un risque abstrait : c'est un document que la société avait elle-même rédigé.**

La règle d'un an n'a pas protégé l'assureur, elle a mesuré sa négligence

L'erreur élémentaire suppose une organisation qui ignorait la règle. La délibération décrit l'inverse. Au jour du contrôle, la politique de durée de conservation de la société prévoyait de garder un an les données de la table de journalisation. Les contrôleurs y ont trouvé des connexions de 2003 et les mots de passe de 8 628 clients enregistrés depuis le 11 juillet 2019. La formation restreinte relève que les constatations faites dans la base démontrent l'absence de mise en œuvre effective de cette politique, et que la durée constatée excède « celle que la société a elle-même définie ».

Le point décisif se trouve dans l'examen des critères de l'amende. Au titre de la négligence (critère b de l'article 83 du RGPD), la formation restreinte retient que la société n'a pas respecté la durée d'un an qu'elle avait elle-même fixée, et conclut qu'elle s'est montrée « à tout le moins, particulièrement négligente ». **La règle écrite n'a pas joué comme une preuve de diligence. Elle a fourni l'étalon qui permettait de mesurer l'écart.**

Le même décalage traverse la gestion des accès. En défense, la société soutenait que l'équipe concernée avait toujours disposé de comptes nominatifs pour l'outil de consultation, et que le compte générique utilisé pendant le contrôle n'était pas représentatif. Le mot de passe administrateur partagé n'a pourtant été désactivé que le 22 avril 2026. Le 18 juillet 2024, la société annonce une première fonction de hachage, sans sel cryptographique (une valeur aléatoire ajoutée à chaque mot de passe avant transformation), que la formation restreinte

qualifie d'obsolète. Une fonction conforme à l'état de l'art n'est en place que le 25 avril 2026, après la signification du rapport de sanction. Vingt et un mois séparent la correction annoncée de la correction effective.

Ce que l'organisation déclare et ce que ses tables enregistrent

> **Théorie professée et théorie d'usage (Chris Argyris et Donald Schön, 1974)**
>
> Dans *Theory in Practice: Increasing Professional Effectiveness* (1974), Argyris et Schön distinguent deux théories de l'action. La théorie professée est celle que les acteurs déclarent suivre et savent énoncer. La théorie d'usage, qui gouverne réellement leur conduite, ne se lit que dans les actes. Argyris l'a transposée aux systèmes d'information en 1982 : « Theories-in-use are the theories of action that actually govern their actions » (les théories d'usage sont celles qui gouvernent effectivement leurs actions). Il y oppose l'*apprentissage en simple boucle*, qui corrige l'erreur sans interroger le programme qui l'a produite, à l'apprentissage en double boucle, qui remet ce programme en question. En 1991, il résume le constat qui fonde l'ensemble : les acteurs « consistently act inconsistently » (agissent constamment de manière incohérente), sans percevoir la contradiction entre les deux théories.

Une politique de conservation, un registre des traitements, des comptes nominatifs déclarés relèvent de la théorie professée : ils disent ce que l'organisation fait, et ils sont rédigés pour être montrés. La théorie d'usage se lit ailleurs, dans l'âge de l'enregistrement le plus ancien d'une table, dans le nombre de personnes qui connaissent un mot de passe administrateur. Pour Argyris, l'écart reste souvent invisible à ceux qui l'abritent. Le dossier ne dit pas ce que savaient les équipes de l'assureur. Il montre que rien ne confrontait la règle aux tables avant l'arrivée des contrôleurs.

La méthode de la formation restreinte est, sur ce point, celle d'Argyris : elle infère la théorie d'usage des traces, non des déclarations. Le paragraphe 60 pose que « l'effectivité de la mise en œuvre d'une politique de durée de conservation des données est le pendant nécessaire de sa définition ». La formule est reprise d'une sanction du 29 octobre 2021, ce qui en fait une doctrine établie plutôt qu'une innovation de circonstance. **Pour le régulateur, la politique écrite n'est pas une preuve. C'est une hypothèse que la base de données confirme ou dément.**

La séquence des corrections relève de la simple boucle : chaque mesure répond au constat précédent, du hachage obsolète de 2024 aux comptes nominatifs créés en 2025 à côté du compte commun, sans réexaminer le dispositif qui laissait la règle sans vérification. La *normalisation de la déviance* de Diane Vaughan (1996), cadre de la chronique du 25 octobre, garde un rôle d'appui : elle décrit comment un écart toléré devient routine. Argyris et Schön expliquent pourquoi cette routine coexistait avec une politique qui affirmait le contraire.

Meta, 2019 : la même table de journalisation, un autre chemin de découverte

Le précédent le plus proche est celui de Meta. Le 21 mars 2019, l'entreprise, alors nommée Facebook, publie une note de son vice-président chargé de l'ingénierie, de la sécurité et de la vie privée, Pedro Canahuati, qui rappelle sa règle : « we “hash” and “salt” the passwords » (les mots de passe sont hachés et salés). La note reconnaît qu'une revue de sécurité de routine a trouvé des mots de passe lisibles dans les systèmes internes, pour des centaines de millions d'utilisateurs, sans abus constaté selon l'entreprise. Le 27 septembre 2024, la Data Protection Commission irlandaise annonce une amende de 91 millions d'euros et un blâme, pour des manquements à la sécurité (articles 5-1-f et 32-1 du RGPD) et à l'obligation de notifier et documenter la violation (articles 33-1 et 33-5). Selon l'autorité, ces mots de passe n'avaient pas été rendus accessibles à des tiers, et son commissaire adjoint, Graham Doyle, rappelle qu'il est admis que « user passwords should not be stored in plaintext » (les mots de passe ne doivent pas être stockés en clair).

Même structure : une règle de hachage professée, des journaux qui enregistrent autre chose, une sanction sans exploitation démontrée. Seul diffère le chemin de découverte. Chez Meta, un contrôle interne a confronté la règle aux systèmes. Chez Macif Vie, la confrontation est venue d'un signalement extérieur, puis d'agents qui ont ouvert les tables. Le même écart apparaît hors des mots de passe : en janvier 2026, la CNIL a sanctionné France Travail de 5 millions d'euros après une intrusion, en relevant que la plupart des mesures de sécurité adéquates avaient été identifiées dans ses analyses d'impact sans être mises en œuvre. L'identité des montants ne vaut pas équivalence : l'amende d'un établissement public relève d'une fourchette plafonnée.

Partout où la règle se contrôle dans le document plutôt que dans la base

Le mécanisme se formule sans nom d'organisation. Une règle de sécurité ou de conservation, rédigée pour attester une conformité et jamais confrontée aux données qu'elle régit, finit par coexister avec des pratiques qui la contredisent. Le jour où un contrôle extérieur mesure l'écart, la règle sert d'étalon à la négligence de son auteur.

Quatre conditions favorisent sa reproduction. La première est la rédaction de documents de conformité pour satisfaire une obligation plutôt que pour piloter. La deuxième est l'absence de propriétaire de la vérification : la fonction juridique écrit la règle, la direction des systèmes d'information exploite les tables, et personne n'est chargé de comparer les deux. La troisième tient aux zones techniques héritées (journaux applicatifs, tables de formulaires, comptes de service), qui échappent aux revues parce qu'aucun projet ne les porte. La quatrième est l'accommodement pratique, comme le compte partagé qui simplifie le travail d'une équipe, toléré tant que la question n'est pas posée.

Les signes sont visibles pour qui regarde les données plutôt que les procédures : des audits qui vérifient l'existence des règles et non leur résultat dans les bases, des corrections qui

commencent par la forme, et l'absence d'incident utilisée comme indicateur de sécurité, alors que la délibération du 12 novembre rappelle qu'elle n'en est pas un.

> **Grille de lecture**
>
> 1. Pour chaque table contenant des données de clients, la date de l'enregistrement le plus ancien est-elle connue, et rapprochée de la durée inscrite dans la politique de conservation ?
> 2. Quelle fonction est chargée de comparer la politique écrite au contenu réel des bases, et à quelle date ce rapprochement a-t-il eu lieu pour la dernière fois ?
> 3. Combien de comptes génériques ou partagés donnent accès aux bases de production, et qui en tient la liste ?
> 4. Les journaux applicatifs contiennent-ils des identifiants ou des secrets, et relèvent-ils de la politique de conservation ?
> 5. Après le dernier contrôle, les mesures correctrices ont-elles été vérifiées dans les données, ou seulement déclarées ?

Ce que diront le Conseil d'État et les délibérations de 2027

La délibération du 12 novembre referme la question laissée ouverte le 25 octobre : un système se sanctionne pour ce qu'il est, avant tout incident. Elle en ouvre une autre. Devant le régulateur, la théorie professée devient la mesure de la théorie d'usage, et une politique écrite mais jamais vérifiée devient la preuve de la négligence. Deux indicateurs permettront de vérifier cette lecture.

Le premier est juridique. La décision peut faire l'objet d'un recours devant le Conseil d'État dans les deux mois suivant sa notification, soit au moins jusqu'en janvier 2027. La société n'a contesté ni la sécurité défaillante ni les durées excessives, mais elle a contesté l'assiette du groupe : un éventuel recours porterait vraisemblablement sur le calcul plutôt que sur le principe. Une décision du Conseil d'État serait observable d'ici novembre 2028.

Le second est réglementaire. Si l'hypothèse est juste, les délibérations de sanction publiées par la CNIL d'ici le 31 décembre 2027 retiendront de nouveau, au titre de la négligence, l'écart entre une durée fixée par l'organisme lui-même et celle constatée dans ses bases. Macif Vie ne se lira plus alors comme une erreur de débutant, mais comme une organisation sanctionnée pour avoir écrit la règle sans la confronter à ses propres tables.

Note méthodologique

Les faits reposent sur la délibération SAN-2026-016 et le communiqué de la CNIL du 18 novembre 2026, recoupés par Next et Silicon.fr, auxquels est attribuée l'identification de

Macif Vie. Next situe en séance la baisse de 9 à 7 millions d'euros, la délibération la rattache à la réponse écrite du rapporteur : l'auteur a retenu la délibération. L'absence de fuite est bornée à ce qu'établissent ces deux documents au 23 novembre 2026, et aucune causalité n'est assumée au-delà de la délibération. La normalisation de la déviance ayant servi de cadre central le 25 octobre, l'auteur a retenu la distinction d'Argyris et Schön, restituée à partir des textes d'Argyris de 1982 et 1991. Recherche de sources, croisement des données et structuration du raisonnement s'appuient sur une assistance par intelligence artificielle. Le choix de l'angle et du cadre théorique, la vérification des sources, les arbitrages et l'établissement du texte final relèvent de l'auteur.

Sources

Décisions et documents d'autorités

Commission nationale de l'informatique et des libertés, formation restreinte, « Délibération de la formation restreinte n° SAN-2026-016 du 12 novembre 2026 prononçant une sanction pécuniaire à l'encontre de la société X », publiée sur Légifrance le 18 novembre 2026, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000055097962

Commission nationale de l'informatique et des libertés, « Conservation des mots de passe clients en clair : la CNIL prononce une sanction de 5 millions d'euros », 18 novembre 2026, https://www.cnil.fr/fr/conservation-des-mots-de-passe-sanction-5-millions-deuros

Commission nationale de l'informatique et des libertés, « Violation de données : sanction de 5 millions d'euros à l'encontre de FRANCE TRAVAIL », 29 janvier 2026, https://cnil.fr/fr/violation-de-donnees-sanction-5millions-france-travail

Presse de référence

Alexandre Laurent, « La CNIL sanctionne Macif Vie à hauteur de 5 millions d'euros pour des mots de passe en clair », Next, 18 novembre 2026, https://next.ink/268231/la-cnil-sanctionne-macif-vie-a-hauteur-de-5-millions-deuros-pour-des-mots-de-passe-en-clair/

La rédaction, « CNIL : Macif Vie écope de 5 millions € d'amende pour ses manquements cyber », Silicon.fr, 18 novembre 2026, mis à jour le 20 novembre 2026, https://www.silicon.fr/data-ia-1372/cnil-macif-vie-ecope-de-5-millions-e-damende-pour-ses-manquements-cyber-230514

Chronique précédente

Alexandre Berge, « Macif Vie : l'écart toléré, jugé avant l'incident », elegartech.fr, 25 octobre 2026, https://elegartech.fr/articles/macif-vie-l-ecart-tolere-juge-avant-l-incident

Cadres théoriques

Chris Argyris, « Organizational Learning and Management Information Systems », DATA BASE, numéro d'hiver-printemps 1982, p. 3-11, consulté le 23 novembre 2026, https://www.uky.edu/~gmswan3/575/Argyris_1982.pdf

Chris Argyris, « Teaching Smart People How to Learn », Harvard Business Review, numéro de mai-juin 1991, consulté le 23 novembre 2026, https://med.uio.no/helsam/studier/evu/samfunnsmedisin-i-spesialistutdanningen-for-leger/2021-h%C3%B8st-litteraturliste/argyris---teaching-smart-people-to-learn.pdf

Parallèle historique

Pedro Canahuati, « Keeping Passwords Secure », Meta, 21 mars 2019, mis à jour le 7 novembre 2019, https://about.fb.com/news/2019/03/keeping-passwords-secure/

Data Protection Commission (Irlande), « Irish Data Protection Commission fines Meta Ireland €91 million », 27 septembre 2024, https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-91-million-fine-of-Meta