LE COIN DU DPO
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Publications de Janvier 2026

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
LE COIN RÉGLEMENTATION	07/01/2026	Renouvellement de la décision d'adéquation du Royaume-Uni au titre du RGPD	Le 19 décembre 2025, la Commission européenne a renouvelé la décision d'adéquation RGPD concernant le Royaume-Uni, ce qui confirme que les données personnelles peuvent continuer à circuler librement et en sécurité entre l'Espace économique européen (« EEE ») et le Royaume-Uni, le cadre britannique offrant des garanties jugées essentiellement équivalentes à celles de l'Union européenne (« UE »). Ce renouvellement intervient après une prorogation technique de 6 mois décidée en juin 2025, le temps pour la Commission de finaliser son évaluation, notamment au regard des évolutions législatives britanniques. Les nouvelles décisions comportent une clause de caducité de 6 ans : elles s'appliquent jusqu'au 27 décembre 2031 avec un réexamen après 4 ans en lien avec le Comité européen de la protection des données (« CEPD ») et un suivi continu des évolutions au Royaume-Uni. Par conséquent, pour les organismes de l'EEE, les transferts vers le Royaume-Uni restent possibles sans clauses contractuelles types ni dérogation au titre des règles de transfert (sous réserve du périmètre de l'adéquation).	Pour information -
LE COIN RÉGLEMENTATION	07/01/2026	Délibération n° SAN – 2025-015 du 22 décembre 2025 à l'encontre de la société NEXPUBLICA FRANCE	Le 22 décembre 2025, la CNIL a sanctionné NEXPUBLICA France (éditeur/prestataire du progiciel PCRM), intervenant comme sous-traitant, d'une amende de 1,7 million d'euros pour manquement à l'article 32 du RGPD, à la suite de violation de données liées à l'accès de tiers via un portail usager (contexte MDPH/action social – handicap).	Appliquer le principe de défense en profondeur afin de renforcer la traçabilité/journalisation

			A la suite de signalements fin 2022, la CNIL a contrôlé la société et a retenu principalement : - Mesures de sécurité non appropriées (art.32) : absence de dispositif de sécurité à la hauteur de la sensibilité des données (données sociale /médico-sociales) et des risques associés ; - Contrôle d'accès et cloisonnement insuffisants : accès indus à des données de tiers via des anomalies/paramétrages du portail ; - Absence de défense en profondeur : vulnérabilité connues et documentées par des audits, avec remédiation jugée tardive ; - Faiblesse de traçabilité/journalisation : difficultés à reconstituer précisément le périmètre des données exposées (non-maîtrise de la réponse à l'incident). La CNIL confirme, une nouvelle fois, qu'un sous-traitant peut être sanctionné directement sur le fondement de l'article 32, des audits défavorables deviennent un élément à charge si la correction n'est pas rapide et traçable.	
LE COIN RÉGLEMENTATION	13/01/2026	Conseil d'Etat, 23 décembre 2025, n°492830, Amazon France Logistique	Le 23 décembre 2025, le Conseil d'Etat a partiellement réformé la sanction CNIL SAN-2023-021 du 27 décembre 2023 relative aux outils de suivi de l'activité des salariés en entrepôt : l'amende a été ramenée de 32 M à 15M €. Il a jugé que la CNIL a commis une erreur d'appréciation en qualifiant d'illicites certains traitements en temps réel : compte tenu de leurs seuils et de finalités opérationnelles reconnues ces indicateurs ne portent pas une atteinte excessive aux droits des salariés et peuvent reposer sur l'intérêt légitime.	- Vérifier les outils de surveillance des salariés et ne les utiliser qu'à des fins organisationnelles, légitimes et proportionnées, non disciplinaires.

			En revanche, le Conseil d'Etat confirme le manquement au principe de minimisation tenant à la conservation indifférenciée de l'ensemble des indicateurs pendant 31 jours, durée jugée non démontrée comme nécessaire au regard des finalités invoquées. La décision ordonne la publication de la réformation dans les mêmes conditions que la publication initiale CNIL et condamne la CNIL à 3 000 € au titre des frais. Ainsi, le CE ne valide pas une surveillance généralisée, mais indique qu'un pilotage en temps réel peut être licite s'il est cadré (seuils, finalités, absence d'intrusion excessive) et documenté, en revanche les points qui restent très exposants sont la minimisation/conservation, la transparence et la sécurité des outils de vidéosurveillance.	- Justifier les durées de conservations
LE COIN RÉGLEMENTATION	14/01/2026	Délibération n°SAN-2026-001 du 8 janvier 2026 prononçant une sanction pécuniaire à l'encontre de la société FREE MOBILE	Le 8 janvier 2026, la CNIL a sanctionné FREE MOBILE d'une amende de 27 millions d'euros à la suite d'une violation de données d'octobre 2024 ayant permis l'accès aux données relatives à plus de 19,4 millions de contrats mobiles, au sein d'un périmètre global d'environ 24,6 millions de contrats. Et elle a assorti sa décision de mesures de mise en conformité, Après contrôle en novembre 2024 et instruction, la CNIL a retenu plusieurs manquements : - Conservation excessive des données (art. 5(1)(e) RGPD) : absence de purge/tri effectifs entraînant une conservation indéfinie de données de contrats résiliés (volumes très importants au-delà des durées annoncées par Free Mobile) ; - Sécurité insuffisantes (art.32 RGPD) : insuffisance de protection des accès et de détention, ayant facilité l'intrusion et l'exfiltration, notamment via l'accès	S'assurer d'un accès distant robuste, d'une détection active des extractions anormales (alertes + blocage) et d'une politique de conservation réellement appliquée (purge/archivage effectif)

			distant / VPN et l'outil interne de gestion abonnés MOBO ; - Information insuffisante des personnes sur la violation (art. 34 RGPD) : communication jugée trop générale ; la CNIL admet un dispositif d'information à « deux niveaux », mais exige que l'email initial contienne des éléments actionnables (risques, mesures prises, recommandations).	
LE COIN RÉGLEMENTATION	14/01/2026	Délibération n°SAN-2026-002 du 8 janvier 2026 prononçant une sanction pécuniaire à l'encontre de la société FREE	Le 8 janvier 2026, le CNIL a sanctionné FREE d'une amende de 15 millions d'euros, dans le cadre de la même cyberattaque d'octobre 2024 que celle de FREE MOBILE (voir ci-dessus) : l'intrusion initiale est passée par FREE MOBILE, puis l'accès aux données « fixe » a été rendu possible via interconnexion des systèmes (clients « convergents »). Environ 5,17 millions de contrats fixes sont concernés. A l'issue du contrôle et de la procédure disjointe en octobre entre les deux affaires FREE et FREE MOBILE, la CNIL a retenu : - Sécurité insuffisante (art.32 RGPD) : exigences renforcées sur les accès distants/nomadisme (authentification robuste) et surtout sur la détection des comportements anormaux sur l'outil de gestion abonnés fixe (SIEBEL) : logs présents mais insuffisamment exploités (alerte/blocage), ce qui a permis une exfiltration massive des données sans détection rapide ; - Information insuffisante des personnes (art. 34 RGPD) mêmes critiques de fond que pour Free Mobile (message initial trop vague, manque d'éléments concrets sur les risques, les mesures	S'assurer que la détection est en temps réel sur les outils clés et que l'exposition des données sensibles est minimisée, l'information aux personnes doit être actionnable dès le premier message. .

			prises et les recommandations), avec un focus attendu lorsque des données bancaires (IBAN) sont en cause. Même lorsqu'une attaque/intrusion provient d'un autre SI du groupe, la CNIL examine l'effectivité des mesures propres à chaque entité, la sécurité active (détection en temps réel et réaction/blocage) devient un standard attendu. L'information doit être immédiatement opérationnelle pour réduire les risques d'exploitation tels que le phishing ou la fraude.	
 LE COIN POUR ALLER PLUS LOIN	19/01/2026	CNIL – Certifications et codes de conduite : la CNIL cartographie le déploiement des outils RGPD en Europe – 14 janvier 2026	Le 14 janvier 2026, la CNIL a mis en ligne deux cartes recensant, à l'échelle européenne, les codes de conduite et certifications RGPD approuvés par les autorités nationales ou par le CEPD depuis l'entrée en application du RGPD, afin de faciliter l'identification des outils de conformités disponibles. La CNIL souligne que ces dispositifs sont des outils opérationnels de conformité (logique d'accountability), visant à harmoniser les pratiques au sein d'un secteur et à apporter des garanties appropriées en protection des données. Ces derniers peuvent notamment être recherchés par pays/domaine d'activité. Ces cartes deviennent un vrai réflexe de veille et de due diligence. Elles permettent d'identifier rapidement quels codes de conduite ou certifications RGPD existent déjà par secteurs/pays, d'en faire un levier contractuel et de bâtir une feuille de route de conformité adossée à des standards reconnus plutôt que de ne partir de rien.	 S'assurer d'identifier les codes/certifications RGPD existants du secteur ou de l'activité
 LE COIN POUR ALLER PLUS LOIN	19/01/2026	Délibération n°2025-131 du 18 décembre 2025 proposant des modalités pratiques de mise en conformité du consentement multi-terminaux et portant modification de la	Le 18 décembre 2025, la CNIL a adopté la délibération n°2025-131, publiée au Journal officiel du 18 janvier 2026, qui complète/modifie sa recommandation « cookies et autres traceurs » (2020-092) en posant un cadre pratique pour le consentement multi-terminaux dans les univers authentifiés (« logués »).	

		recommandation n°2020-092 du 17 septembre 2020 dite « cookies et autres traceurs »	La CNIL y précise notamment : - Le périmètre : le consentement multi-terminaux qui s'applique à tous les environnements utilisés avec ce compte - Le caractère optionnel : le dispositif est facultatif - L'information renforcée : l'utilisateur doit être informé, avant de choisir, que ses préférences seront appliquées à tous ses terminaux connectés au compte ; et lors de la connexion depuis un nouveau terminal, un bandeau éphémère doit rappeler la portée des choix - La gestion des contradictions (avant/après connexion : si, avant de se connecter, l'utilisateur exprime sur un terminal des choix différents de ceux de son « compte », la CNIL admet deux modalités : le dernier choix écrase les préférences du compte et devient valable sur tous les terminaux ou bien, les préférences du compte prévalent avec une information claire sur ce qui s'applique. Ainsi, la CNIL « autorise » un consentement unique cross-device (en univers logué) mais en échange d'exigences très concrètes de transparence et de gestion loyale des contradictions éventuelles. En effet, le consentement unique cross-device ne doit pas être un simple moyen de « réduire les bannières d'information » au détriment du droit au refus.	S'assurer que le consentement en cross-device est transparent et clair et symétrique (refuser/retirer aussi simple qu'accepter), avec une gestion claire des contradictions avant/après connexion.
LE COIN RÉGLEMENTATION	23/01/2026	EN CONSULTATION - EDPB - Recommendations 1/2026 on the Application for Approval and on the elements and principles to be found in Processor Binding Corporate Rules (Art. 47 GDPR) - January 2026	EN CONSULTATION jusqu'au L'EDPB a publié son projet de recommandations 1/2026 sur les règles d'entreprise contraignantes (BCR processor ou BCR-P) au titre de l'article 47 du RGPD : elles mettent jour le référentiel historique du G29 et fournissent un cadre harmonisé pour déposer une demande d'approbation et rédiger le contenu minimal attendu des BCR-P.	Pour information

Icônes « Quelles actions ? » by Adrien Coquet

		EDPB = European Data protection Board ou Comité européen de la protection des données	Le texte rappelle surtout que les BCR-P encadrent les transferts intra-groupes lorsqu'un groupe agit comme sous-traitant pour des responsables de traitement externes, et précise les exigences pour : opposabilité, responsabilité d'une entité UE pour les entités hors UE, encadrement des transferts ultérieurs et mécanismes d'effectivité.	
LE COIN RÉGLEMENTATION	23/01/2026	Délibération de la formation restreinte n° SAN-2025-017 du 30 décembre 2025 concernant la société X	Le 30 décembre 2025, la CNIL a sanctionné une enseigne de distribution (décision anonymisée) d'une amende de 3,5 millions d'euros pour plusieurs manquements au RGPD et à la loi informatique et libertés (« LIL »), liés notamment à l'usage des données de son programme de fidélité pour la publicité ciblée sur un réseau social. L'autorité reproche principalement à l'enseigne d'avoir alimenté, de 2018 à 2024, un dispositif de ciblage publicitaire sur réseau social en transmettant régulièrement les adresses email et/ou numéros de téléphone de ses membres afin de constituer des audiences et d'étendre la diffusion à des profils similaires, sans consentement spécifique et suffisamment éclairé. Pour la CNIL, un consentement donné pour de la prospection par email/sms ne peut pas, à lui seul, couvrir la publicité ciblée via une plateforme tiers impliquant une mise en correspondance de données. La décision relève également : une information insuffisante, l'absence d'AIPD pour un traitement à grande échelle avec croisement de données, le défaut de sécurité sur la gestion des mots de passe, ainsi que des irrégularités en matière de cookies/traceurs (dépôt avant choix et lecture malgré refus). Cette sanction rappelle ainsi que les mécanismes de matching/looalike sur réseaux sociaux exigent un consentement spécifique, explicite et traçable, distinct du	- En cas de ciblage publicitaire via les réseaux sociaux, s'assurer du recueil d'un consentement spécifique distinct de l'opt-in email/sms et de la réalisation d'une AIPD en cas de traitement à grande échelle/croisement

			simple opt-in à la prospection email/sms et une information claire sur la transmission à la plateforme.	⇨ Vérifier l'utilisation de cookies nécessitant le consentement, et leur dépôt
LE COIN RÉGLEMENTATION	23/01/2026	EDPB - Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive ("LED") under Article 62 LED - January 2026	En janvier 2026, l'EDPB a publié sa contribution à l'évaluation par la Commission de la Directive « Law renforcement » (LED – Directive 2016/680) dans le cadre de l'évaluation périodique prévue par le texte. L'EDPB met surtout en avant plusieurs messages clés : - La valeur ajoutée de la LED comme cadre harmonisé pour la protection des données en contexte répressif, - Un besoin de clarification du champ/frontière LED/RGPD (notamment avec les systèmes informatiques multi-finalités et les grands systèmes européens interopérables) ; - L'impact des nouvelles technologies (IA, big data) qui impose une application stricte des principes de proportionnalité/nécessité ; - Enjeux de droits des personnes, coopération/transferts, rôle des DPO et ressources encore insuffisantes des autorités de contrôles.	Pour information
LE COIN RÉGLEMENTATION	26/01/2026	Délibération n°2025-132 du 18 décembre 2025 portant modification du règlement intérieur de la Commission nationale de l'informatique et des libertés	Cette délibération de la CNIL, publiée au Journal officiel du 23 janvier 2026, amende le règlement intérieur de la CNIL en simplifiant et actualisant, notamment, le chapitre consacré aux formalités préalables. Elle formalise un process des formalités préalables : vérification de la complétude du dossier, demande de pièces	Pour information

			manquantes (par mail ou papier) avec possibilité de fixer un délai, et clôture dudit dossier en l'absence de réponse. Elle encadre également la vie du dossier : en cas d'erreur sur le régime choisi par le responsable de traitement, l'organisme est invité à refaire la bonne formalité, et en cas de modification ou suppression du traitement le RT doit le notifier et peut devoir repasser par une formalité si la modification est substantielle, un récépissé lui est délivré dans le cas d'une suppression.	
LE COIN RÉGLEMENTATION	29/01/2026	EDPB - Document setting forth a Cooperation Procedure for the Authorisation of Contractual Clauses under Article 46(3)(a) GDPR and for the Adoption of Standard Contractual Clauses under Article 46(2)(d) GDPR - January 2026	Le document adopté par l'EDPB le 22 janvier 2026 établit une procédure commune permettant aux autorités de contrôle de l'EEE de coopérer lors de l'autorisation de clauses contractuelles ad hoc au titre de l'article 46 (3)(a) du RGPD et de l'adoption de clauses contractuelles types (« SCC ») par une autorité nationale, en vertu de l'article 46(2)(d). Deux objectifs sont visés par le texte : assurer une application cohérente des mécanismes de transfert international de données entre Etats membres et en termes de rationalisation, d'éviter la duplication des travaux lorsque des clauses sont utilisées dans plusieurs juridictions. La procédure se caractérise par : - Coopération informelle entre autorités de contrôle pour examiner les clauses avant toute étape formelle - Identification d'une autorité chef de file, responsable de coordonner l'analyse et la circulation des commentaires - Avis de l'EDPB : lorsque cela est nécessaire, un avis formel est rendu sous l'article 64 RGPD pour garantir une cohérence européenne	Pour information

			- La décision finale demeure de la compétence de l'autorité national responsable du dossier, conformément aux articles 46(3)(a) et 46 (2)(d). Ce document s'inscrit ainsi dans les travaux réguliers de l'EDPB pour assurer une application cohérente du RGPD et compléter les ressources disponibles en matière de mécanismes de transfert.	
LE COIN RÉGLEMENTATION	29/01/2026	EDPB - Rules of Procedure for the "Informal Panel of EU DPA's according to the EU-US. Data Privacy Framework – version 2.0 – January 2026	Ce document met à jour les règles de fonctionnement du Panel informel des autorités de protection des données (« DPAs ») de l'UE dans le cadre UE-US. Data Privacy Framework (« DPF »). Il vise à assurer une coordination cohérente entre DPAs lorsqu'elles traitent des plaintes ou renvois, liés au DPF. Le texte organise : - La compétence du Panel pour coordonner le traitement des plaintes liées au DPF - La désignation d'une DPA chef de file et de co-reviewers chargés de l'analyse conjointe - Les obligations de la DPA qui reçoit une plainte, du Lead DPA et des co-reviewers - Les modalités de coopération et de communication entre DPAs pour garantir un traitement harmonisé des dossiers relevant du DPF. Les modalités de coopération et de communication entre DPAs pour garantir un traitement harmonisé des dossiers relevant du DPF. L'objectif est donc d'assurer une réponse cohérente et uniforme des autorités européennes dans la gestion des plaintes transatlantiques liées au Data Privacy Framework.	Pour information

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	29/01/2026	EDPB - EU-U.S. Data Privacy Framework F.A.Q. for European businesses - version 2.0 - January 2026	L'EDPB a mis à jour la FAQ relative au Data Privacy Framework (« DPF »), version entreprises, initialement publiée en 2024.La version de 2026 n'apporte pas de modification substantielle au document. Elle précise notamment, s'agissant des transferts de données RH, les conditions exactes dans lesquelles une entreprise américaine peut recevoir ces données, y compris l'obligation éventuelle de coopérer avec les autorités européennes de protection des données et d'être explicitement informée que le transfert inclut des données HR. La version de 2026 clarifie également la vérification du statut de certification active via la « DPF List » et harmonise la structure et la terminologie du document. Globalement, les obligations de vérification préalable, de respect du RGPD (base légale, information des personnes, accord de sous-traitance au titre de l'article 28) et de responsabilité en cas de recours à des sous-traitants demeurent inchangées, mais sont présentées de manière plus structurée et précise.	Pour information
LE COIN RÉGLEMENTATION	05/12/2025	EDPB - EU-US Data Privacy Framework FAQ for European individuals - version 2.0 - January 2026	L'EDPB a mis à jour la FAQ relative au Data Privacy Framework (« DPF »), initialement publiée en 2024.La version de 2026 n'apporte pas de modification substantielle au document, mais introduit plusieurs clarifications procédurales. Elle précise notamment que les entreprises certifiées doivent répondre aux plaintes dans un délai de 45 jours calendaires. Elle indique également de manière explicite que l'EDPB n'est pas l'autorité compétente pour recevoir directement les plaintes, celles-ci devant être adressées à une autorité nationale de protection des données.	Pour information

LE COIN RÉGLEMENTATION	29/01/2026	EDPB – EU-US Data Privacy Framework Template Complaint Form for Submitting Complaints to EU DPAs related to the Data Privacy Framework Principles – version 2.0 – January 2026	L'EDPB a mis à jour le formulaire de plainte relatif au DPF. L'EDPB n'apporte pas de modification substantielle au mécanisme de traitement des plaintes, mais renforce la clarté, la pédagogie et la structuration du document. Il est désormais expressément précisé que l'EDPB n'est pas l'autorité compétente pour recevoir les plaintes et que celles-ci doivent être adressées à une autorité nationale de protection des données. En outre, les questions du formulaire sont reformulées et simplifiées, en invitant le plaignant à détailler davantage l'atteinte alléguée et, si possible, à identifier les principes du DPF concernés. La nouvelle version de la FAQ introduit également un glossaire détaillé des notions clés ainsi qu'une section d'informations générales expliquant l'objet du formulaire, son champ d'application et les cas dans lesquels il ne doit pas être utilisé (notamment pour les questions liées à la sécurité nationale ou à des violations du RGPD sans lien avec le DPF). Enfin, elle clarifie la présentation des règles relatives à la protection des données du plaignant et au transfert éventuel de ses données vers les autorités américaines, sans modifier les garanties de fond.	Pour information
LE COIN RÉGLEMENTATION	29/01/2026	EDPB-EDPS – Joint opinion 1/2026 on the Proposal for a regulation as regards the simplification of the implementation of harmonized rules on artificial intelligence (Digital Omnibus on AI) – January 2026 *EDPS = European Data Protection Supervisor*	L'EDPB et l'EDPS ont adopté un avis conjoint sur la proposition de la Commission européenne visant à simplifier la mise en œuvre du règlement sur l'intelligence artificielle (« IA ») (AI Act), notamment par des ajustements techniques destinés à améliorer l'applicabilité des règles harmonisées existantes. Leur position soutient les objectifs de simplification, tout en soulignant que celle-ci ne doit jamais affaiblir la protection des droits fondamentaux et des données personnelles. Les autorités soutiennent l'extension ciblée de la base légale permettant de traiter des catégories particulières de données à des fins de détection et correction des biais. Elles insistent toutefois pour que cette possibilité reste strictement	Pour information

		ou Contrôleur européen de la protection des données en français	encadrée, limitée aux cas où le risque lié au biais est suffisamment sérieux et ou le traitement est d'une nécessité stricte, pour éviter les dérives. En revanche, elles s'opposent à la suppression de l'enregistrement des systèmes non classés à haut risque : cette transparence est indispensable pour permettre une supervision efficace et éviter les erreurs de classification. S'agissant des sandboxes d'IA, les sandboxes européens sont soutenus, à condition que les autorités de protection des données participent systématiquement, afin d'assurer la cohérence avec le RGPD. Les autorités demandent également une clarification du rôle du AI Office, pour éviter une centralisation excessive et garantir que les autorités nationales conservent de véritables pouvoirs d'enquête et d'intervention. Elles recommandent de maintenir l'obligation de formation (« AI literacy ») à la charge des fournisseurs et déployeurs, plutôt que d'en faire une simple mesure d'encouragement afin de garantir une utilisation responsable de l'IA. Par ailleurs, elles expriment des réserves quant au report proposé des règles pour les systèmes à haut risque et invitent à limiter tout retard, notamment pour les exigences de transparence.	

LE COIN DU DPO
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

 LE COIN RÉGLEMENTATION	29/01/2026	Délibération n°SAN-2026-003 du 22 janvier 2026 prononçant une sanction pécuniaire à l'encontre de l'opérateur France Travail	Le 22janvier 2026, la CNIL a prononcé une sanction de 5 millions d'euros à l'encontre de l'opérateur public France Travail (ex-Pôle emploi), pour manquement grave à l'obligation de sécurité prévue à l'article 32 du RGPD. France Travail a subi une intrusion informatique majeure : des attaquant ont utilisé des techniques d'ingénierie sociale pour usurper les comptes de conseiller Cap Emploi. Cette attaque a permis l'accès aux données de millions de personnes, inscrites au cours des 20 dernières années, dont numéros de sécurité sociale et coordonnées. A ce titre, la CNIL relève des défaillances structurelles dans les mesures de sécurité : authentification insuffisante des conseillers Cap Emploi, journalisation lacunaire empêchant la détection rapide d'activité anormales, droit d'accès excessivement étendus, permettant à des agents de consulter des données de personnes non suivies, absence de mesure pourtant identifiées dans des analyses d'impact antérieures. Ces faiblesses ont rendu l'attaque largement facilitée.	 - Vérifier les mesures de sécurité essentielles (authentifications, journalisation) - Vérifier la mise en œuvre des mesures identifiées lors des AIPD tout en documentant leur mise en œuvre
 LE COIN POUR ALLER PLUS LOIN	29/01/2026	ANS-Assurance maladie – Mon espace santé : du dossier médical à la prévention personnalisée – Janvier 2026	L'Agence du numérique en santé (« ANS ») et l'Assurance maladie ont annoncé le 29 janvier 2026 une nouvelle étape stratégique pour Mon espace santé, qui évolue d'un simple espace sécurisé de stockage et partage des données médicales vers un outil central de prévention personnalisée et de coordination des soins. Le service ne se limite plus au Dossier médical partagé : de nouvelles fonctionnalités permettent une prévention active adaptée au profil de chaque usager, notamment via des rappels ciblés, un agenda santé, des auto-questionnaires pour préparer des bilans de prévention.	 Pour information

			Ils proposent également des parcours spécifiques déjà opérationnels : parcours grossesse et carnet de santé numérique de l'enfant. Mon espace santé s'appuie sur un catalogue de 45 services numériques référencés, sélectionnés selon des critères exigeants de sécurité, d'éthique et d'interopérabilité. Avec le consentement explicite de l'usager, les données pourront être réutilisées par des services de confiance, renforçant le rôle de l'outil dans la coordination du parcours de soin. L'objectif affiché est de faire de Mon espace santé un outil central de la médecine préventive française, et d'atteindre notamment, 40 millions d'utilisateurs d'ici 2027.	