LE COIN DU DPO
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Publications de mars 2026

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN RÉGLEMENTATION	04/03/2026	CNIL – Tables informatiques et libertés – Edition 2025	Les Tables informatiques et libertés 2025 publiées par la CNIL constituent un recueil structuré de sa doctrine, rassemblant sous forme de résumés l'essentiel de la jurisprudence, des décisions, et des positions internes de la CNIL en matière de protection des données personnelles. Ce document vise à combler un manque : si la jurisprudence nationale et européenne est accessible, la pratique décisionnelle de la CNIL, y compris de nombreuses décisions non publiées, restait jusque-là partiellement invisible aux professionnelle les Tables permettent donc de rendre transparente cette doctrine interne afin de comprendre l'application concrète du RGPD et de la loi Informatique et libertés. Le document, organisé selon un plan thématique (sécurité, consentement, droit des personnes, transferts de données, etc.) couvre un périmètre large, intégrant notamment les décisions de la CNIL, les arrêts des juridictions suprêmes nationales (Conseil d'Etat et Cour de cassation), les décisions européennes et les lignes directrices du CEPD.	 Pour information
 LE COIN POUR ALLER PLUS LOIN	05/03/2026	EN CONSULTATION - CNIL / HAS – Projet de guide « accompagner le bon usage des systèmes d'intelligence artificielle en contexte de soins »	En consultation jusqu'au 16 avril 2026. Ce projet de guide, mis en consultation publique, vise à outiller les établissements et professionnels de santé pour déployer des systèmes d'intelligence artificielle (« SIA ») en contexte de soins de manière conforme et sécurisée, il s'inscrit dans le cadre du 6e cycle de certification des établissements de santé piloté par la Haute Autorité de santé (« HAS »), officiellement lancé le 1er septembre 2025 (cycle 2025-2030, référentiel HAS version 2025).	 ⇨ Mettre en place une véritable gouvernance SIA (responsabilités, processus de

			Il poursuit deux objectifs : clarifier les obligations applicables aux professionnels de santé, établissements et structure de soins et proposer des bonnes pratiques de déploiement et d'usage des SIA. Le guide est structuré en fiches couvrant tout le cycle de vie : gouvernance, acquisitions/contractualisation, adéquation au contexte local, formation/acculturation, organisation des soins, conditions d'utilisation, information des personnes, contrôles humain/décision automatisée, traçabilité, maintenance et fin de vie/désinstallation, avec une fiche dédiée aux IA génératives. Il distingue particulièrement le déployeur et insiste sur une démarche graduée (recommandations « standard », « avancées » et réflexes indispensables).	validation, contrôle humain, traçabilité et suivi des performances, etc.) ⇨ Sécuriser l'amont contractuel et l'aval opérationnel : clauses, formation des utilisateurs, information des patients, etc.
LE COIN RÉGLEMENTATION	05/03/2026	EDPB – Data brokers market study – March 2026	Cette étude (programme Support Pool of experts) a été réalisée à la demande de l'autorité belge (BE SA) pour cartographier l'écosystèmes des « data brokers » (courtier en données) –ayant une (présumée) implantation principale en Belgique, et proposer une méthodologie réutilisable par d'autres autorités dans l'UE. Les data brokers sont des acteurs qui collectent, agrègent, enrichissent et revendent/partagent des données à des tiers, généralement à des fins de profilage, ciblage, prospection, etc. L'étude retient une approche pragmatique : en pratique, peu d'acteurs remplissent entièrement une définition « stricte » du courtage de données ; l'étude propose donc une définition et des critères de sélection, puis une typologie élargie permettant de classer les acteurs qui ne satisfont pas aux critères. Sur la méthode d'identification, l'étude montre que la piste des codes d'activités (NACABEL – équivalent du code APE en France permettant de classer les entreprises par secteur	Pour information

			d'activité) est peu efficace en raison des déclarations auto-reportées. En revanche, une recherche par mots-clés et des investigations de la présence en ligne permettent de constituer une « liste préliminaire » des candidats potentiels, à partir de laquelle les véritables acteurs sont ensuite filtrés et qualifiés. Elle aboutit à huit catégories (du courtier pur à des intermédiaires/plateformes proches) et associe à chaque catégorie une appréciation initiale du risque : risque de non-conformité RGPD et d'exposition des données.	
LE COIN RÉGLEMENTATION	11/03/2026	CNIL – Règlement sur la gouvernance des données : FAQ sur les organisations altruistes des données reconnues dans l'Union européenne – Mars 2026	La CNIL présente le statut d'organisation altruiste en matière de données reconnues dans l'Union européenne crée par le Data Governance Act : il s'agit d'entités qui facilitent la mise à disposition volontaire de données (personnelles ou non) pour des finalités d'intérêt général et non lucratives, dans un cadre de confiance. Le statut est optionnel et repose sur un enregistrement volontaire, en contrepartie, l'organisme altruiste en matière de données (« OAD ») peut utiliser un logo européen associé à un QR code renvoyant au registre public des OAD reconnues. La FAQ détaille les conditions d'enregistrement : être une personne morale poursuivant des objectifs d'intérêt général, exercer à but non lucratif et être juridiquement indépendante de structures lucratives, et organiser l'altruisme via une structure fonctionnellement distincte. Elle précise aussi que l'exigence de conformité à un « recueil de règles » européen est, à ce stade, différemment applicable faute de recueil adopté. La CNIL rappelle qu'elle est autorité compétente en France pour l'enregistrement et indique la modalité pratique de dépôt (par courriel). Sur le plan opérationnel, la CNIL donne des repères : formes juridiques «propices » (reconnaissance d'utilité publique (RUP), groupement d'intérêt public (GIP) et mise en garde	⇨ Qualifier le modèle avant toute demande d'enregistrement OAD ⇨ Sécuriser la conformité : clauses art.28 et interdiction de réutilisation par les prestataires, politique de redevance proportionnée

			contre les structures sans personnalité juridique (ex. consortium) ; possibilité de recourir à un sous-traitant, sous réserve d'un contrat et d'une interdiction d'usage pour compte propre ; possibilité de dégager des bénéfices mais interdiction de distribution, redevances possibles mais devant rester proportionnées, compensations possibles aux contributeurs mais plafonnées aux coûts de mise à disposition.	
LE COIN RÉGLEMENTATION	11/03/2026	EDPS – Formal comments on the draft Commission Implementing Regulation laying down rules for the application of Regulation (EU) 2024/1689 as regards the establishment, development, implementation, operation and supervision of AI regulatory sandboxes – March 2026	L'EDPS commente le projet de règlement d'exécution de la Commission européenne pris sur le fondement de l'AI Act afin de fixer des règles communes et des modalités détaillées de création, fonctionnement et supervision des bacs à sables réglementaires IA (AI regulatory sandboxes). Sur la gouvernance du texte, l'EDPS demande une correction formelle : le projet mentionne une consultation du CEPD alors que la demande d'avis est adressée à l'EDPS ; il recommande donc d'ajuster le considérant concerné. Sur la sélection des projets, l'EDPS estime que les critères doivent intégrer plus explicitement : (i) les objectifs et le périmètre du projet (tels qu'exposés dans le « sandbox plan »), et (ii) la nécessité d'impliquer d'autres autorités pertinentes, dont les autorités de protection des données. Il critique aussi le critère de viabilité économique : difficile à apprécier pour une autorité publique et non prévu par l'AI Act ; s'il est maintenu, il devrait être objectivé. Sur la protection des données, l'EDPS salue l'idée que l'autorité de protection des données soit associée/supervise lorsque des données personnelles sont traitées dans le cadre du bac à sable réglementaire, mais recommande d'exiger que le « sandbox plan » précise le périmètre du traitement, les catégories de données et les garanties. Il insiste aussi sur un point clé de sécurité juridique : même en bac à sable, une base légale valable doit exister au titre du RGPD/EUDPR (règlement 2018/1725), l'AI Act n'emporte pas la base légale data, le fait	Pour information

			d'être en mode bac à sable n'autorise pas automatiquement la collecte/usage de données personnelles. Enfin, l'EDPS propose de clarifier le régime applicable aux bacs à sable réglementaire qu'il pourrait établir pour les institutions de l'UE et encourage une coopération plus explicite entre autorités compétentes et autorités chargées de protéger les droits fondamentaux, dans la logique de suspension d'activités en cas de risque.	
LE COIN RÉGLEMENTATION	12/03/2026	EDPB-EDPS – Joint Opinion 3/2026 on the Proposal for a European Biotech Act – March 2026	L'avis conjoint de l'EDPB et de l'EDPS porte sur la proposition de l'European Biotech Act (règlement européen sur les biotechnologies), visant à renforcer la compétitivité du secteur biotech/biomanufacturing, notamment via des mesures en santé et des ajustements de textes (dont le règlement essai cliniques). Les autorités soutiennent l'objectif de simplification et d'harmonisation, mais insistent : la simplification doit accroître la sécurité juridique sans abaisser le niveau de protection RGPD/EUDPR pour les données de santé. Sur les essais cliniques, plusieurs clarifications sont demandées : - préciser les rôles responsables de traitements : sponsor/investigateurs, seul ou conjoint ; - limiter la portée de la durée minimale de conservation aux seules données du dossier principal de l'essai clinique (clinical trial master file – CTMF) ; - mieux expliciter l'objectif et l'encadrement des réutilisations de données pour d'autres essais ou pour la recherche ; - renforcer le recours à la pseudonymisation lorsque l'identification directe n'est pas nécessaire. Le texte traite aussi des dispositifs de type bacs à sables réglementaires et de l'usage de l'IA dans les essais cliniques : l'EDPB et l'EDPS demandent d'éviter les zones grises	Pour information

			(supervision, coopération entre autorités) et de clarifier que les obligations spécifiques « IA dans les essais cliniques » s'appliquent en plus des obligations de l'IA Act ; ils recommandent également que l'EMA coopère avec l'EDBP pour les lignes directrices pertinentes lorsqu'elles touchent à la protection des données. Enfin, côté prévention des mésusages (biodefense), ils appellent à cadrer strictement les données collectées lors de la vérification du besoin légitime afin d'éviter des collectes disproportionnées.	
LE COIN RÉGLEMENTATION	13/03/2026	ANSSI – Panorama de la cybermenace - 2025	L'ANSSI décrit une menace toujours élevée : 3 586 événements traités en 2025, dont 1 366 incidents ; les secteurs les plus touchés portés à sa connaissance sont l'éducation/recherche, les ministères/collectivités, la santé et les télécoms. Le rapport souligne l'érosion des frontières entre acteurs étatiques et cybercriminels (partage d'outils, adoption croisée de pratiques) et une cybercriminalité dynamique (rançongiciels, exfiltration). Les tendances techniques marquantes incluent l'exploitation de vulnérabilité, en particulier sur les équipements de bordure (composants placés à la frontière système d'information (SI)/internet : pare-feu, VPN, passerelles web/mail), et l'augmentation des risques liés à la chaîne d'approvisionnement et aux environnements cloud. Le panorama relève aussi la persistance d'actions de déstabilisation dans un contexte géopolitique durablement tendu.	Pour information

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	18/03/2026	CNIL – Recommandation sur le déploiement d'un serveur mandataire web filtrant	La CNIL a publié une recommandation pour encadrer le déploiement, par les employeurs, d'un proxy web filtrant (filtrage d'URL, détection / blocage de contenus malveillants) afin de concilier cybersécurité et RGPD, et éviter la surveillance excessive des salariés. Elle rappelle que la base légale la plus fréquente est l'intérêt légitime (avec mise en balance), et que « l'obligation légale » n'est mobilisable que si un texte impose explicitement le dispositif, l'obligation générale de sécurité du RGPD ne suffisant pas. Le cœur du texte porte sur la minimisation des données : - ne journaliser que ce qui est nécessaire : identité, IP, tout ou partie de l'URL, horodatage, catégorie, action, - limiter les données remontées à l'éditeur au nom de domaine, et - encadrer strictement le déchiffrement HTTPS : liste d'exceptions, pas de conservation du contenu en clair sauf détection d'une charge malveillante. La CNIL fixe des repères de conservation des logs : - en principe 6 mois à 1 an, au-delà justification nécessaire, - exige une information individuelle : charte / règlement intérieur, traçabilité de la remise et - attire l'attention sur les risques spécifiques des solutions SaaS.	⇨ Documenter le déploiement : base légale + mise en balance, AIPD si nécessaire, politique de conservation et information individuelle

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	18/03/2026	EDPS - Towards trustworthy AI in the EU public administration: The EDPS Compass for its new role under the AI Act 2026-2027 - March 2026	Ce document fixe la feuille de route 2026-2027 de l'EDPS pour sa nouvelle mission issue de l'AI Act : l'EDPS devient autorité de surveillance du marché pour les systèmes IA mis en service ou utilisés par les institutions/organes/agences de l'UE, et organisme notifié pour certaines évaluations de conformité de systèmes d'IA à haut risque. Ce document d'orientation décrit comment l'EDPS entend rendre cette supervision opérationnelle : articulation entre supervision ex ante (conformity assessment) et ex post (market surveillance), mise en place de mécanismes de coopération avec les institutions de l'UE et renforcement de ses capacités interne tout en garantissant l'indépendance requise compte tenu du cumul des rôles. La stratégie est structurée autour de quatre piliers : supervision des IA des institutions de l'UE, contribution à la gouvernance de l'AI Act, renforcement des capacités des institutions de l'UE (réseaux, partage de connaissance, etc.), et engagement international et échange de bonnes pratiques.	Pour information
LE COIN RÉGLEMENTATION	18/03/2026	CNIL – Règlement sur la gouvernance des données – FAQ sur les organisations altruistes des données reconnues dans l'UE	La CNIL présente le statut d'organisation altruiste en matière de données reconnues dans l'Union européenne crée par le Data Governance Act : il s'agit d'entités qui facilitent la mise à disposition volontaire de données (personnelles ou non) pour des finalités d'intérêt général et non lucratives, dans un cadre de confiance. Le statut est optionnel et repose sur un enregistrement volontaire, en contrepartie, l'organisme altruiste en matière de données (« OAD ») peut utiliser un logo européen associé à un QR code renvoyant au registre public des OAD reconnues. La FAQ détaille les conditions d'enregistrement : être une personne morale poursuivant des objectifs d'intérêt général, exercer à but non lucratif et être juridiquement indépendante de structures lucratives, et organiser l'altruisme via une	⇨ Qualifier le modèle avant toute demande d'enregistrement OAD ⇨ Sécuriser la conformité : clauses art.28 et interdiction de réutilisation par les prestataires,

			structure fonctionnellement distincte. Elle précise aussi que l'exigence de conformité à un « recueil de règles » européen est, à ce stade, différemment applicable faute de recueil adopté. La CNIL rappelle qu'elle est autorité compétente en France pour l'enregistrement et indique la modalité pratique de dépôt (par courriel). Sur le plan opérationnel, la CNIL donne des repères : formes juridiques «propices » (reconnaissance d'utilité publique (RUP), groupement d'intérêt public (GIP) et mise en garde contre les structures sans personnalité juridique (ex. consortium) ; possibilité de recourir à un sous-traitant, sous réserve d'un contrat et d'une interdiction d'usage pour compte propre ; possibilité de dégager des bénéfices mais interdiction de distribution, redevances possibles mais devant rester proportionnées, compensations possibles aux contributeurs mais plafonnées aux coûts de mise à disposition.	politique de redevance proportionnée
LE COIN RÉGLEMENTATION	19/03/2026	Conseil d'Etat 20 mars 2026 – 503159, 504171 - HDH	Le Conseil d'Etat (« CE ») rejette deux recours dirigés contre la délibération CNIL n°2025-014 du 13 février 2025 qui autorise l'Agence européenne des médicaments (« EMA »), à mettre en œuvre, pendant trois ans, un traitement automatisé de données de santé pour des études de prévalence et d'incidence de pathologies dans la population française, dans le cadre du réseau DARWIN EU. Le contentieux portait principalement sur le risque de transfert vers les Etats-Unis lié à l'hébergement par Microsoft Ireland. Le CE souligne que l'autorisation CNIL a pour objet le traitement de données hébergées en France et n'autorise pas un transfert de données de santé vers les Etats-Unis ; dès lors, les requérants ne peuvent utilement contester la décision d'adéquation UE-USA de 2023 ni invoquer la règle prohibant les transferts de données de santé hors UE.	Pour information

			S'agissant des seuls flux identifiés comme susceptibles d'impliquer un pays tiers, le CE retient que d'éventuels transferts portent sur des données techniques d'usage (connexion d'utilisateurs), sans données de santé, et qu'ils reposent sur des clauses contractuelles types. Il juge enfin que, malgré la sensibilité des données et l'hypothèse de demandes d'accès par des autorités américaines via la société mère, les mesures de sécurité et d'encadrement (pseudonymisation, limitation de conservation, certification HDS), justifient l'appréciation de la CNIL, et il écarte toute saisine préjudicielle de la Cour de justice de l'Union européenne.	
 LE COIN RÉGLEMENTATION	19/03/2026	Délibération n°SAN-2026-004 du 4 mars 2026 relative à l'injonction prononcée à l'encontre de la société KASPR par la délibération n° SAN-2024-020 du 5 décembre 2024	La formation de la CNIL constate que la société KASPR a exécuté l'injonction prononcée le 5 décembre 2024. L'injonction portait sur plusieurs manquements : - licéité : cesser certaines collectes liées à LinkedIn, - conservation : mettre fin au renouvellement automatique d'un durée de cinq ans, - transparence : information dans une langue comprise, et - droit d'accès : réponse et information sur la source des données. KASPR justifie sa mise en conformité par des mesures fortes : effacement de sa base, arrêts de la collecte sur LinkedIn, modification du mécanisme de conservation, information des personnes dans toutes les langues officielles de l'UE, et traitement des demandes d'accès visées. Après échanges complémentaires avec les services de la CNIL, la formation restreinte retient que l'injonction a été satisfaite dans le délai imparti.	 Pour information

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	19/03/2026	CNIL – CEF – CEPD lance une action coordonnée concernant les obligations de transparence et d'information *CEPD ou EDPB = European Data protection Board ou Comité européen de la protection des données*	Le Comité européen de la protection des données (« CEDP ») lance, pour 2026, la 5e action du Coordinated Enforcement Framework (CEF) centrée sur le respect par les responsables de traitement des obligations de transparence et d'information prévues par les articles 12, 13 et 14 du RGPD. L'enjeu est concret : vérifier si les personnes reçoivent une information accessible, complète et compréhensible sur les traitements, conditions préalables à l'exercice effectif des droits. L'initiative vise à harmoniser les pratiques de contrôle : 25 autorités participeront et contacteront des organismes de différents secteurs, soit par des enquêtes formelles, soit par des démarches de type questionnaires (démarche fact-finding). Au second semestre 2026, les autorités mettront en commun leurs constats afin d'établir un rapport consolidé adopté par le CEPD, susceptible d'entraîner des suites ciblées au niveau national et européen.	Pour information
LE COIN RÉGLEMENTATION	19/03/2026	CJUE – 19 mars 2026 – Comdribus – C-371/24 – Collecte de données biométriques par une autorité de police CJUE = Cour de justice de l'Union européenne	La CJUE a pu juger que la collecte, par une autorité de police, de données biométriques (notamment empreintes et photographies) dans le cadre d'une enquête pénale relève du régime de la directive (UE) 2016/680 et ne peut être admises que si elle répond à une nécessité absolue (strictement nécessaire au regard des circonstances). La Cour refuse une logique de relevé « automatique » : la mesure ne peut pas être imposée de façon systématique et doit être clairement motivée, afin de permettre un contrôle effectif (y compris juridictionnel) sur la réalité de la nécessité et de la proportionnalité.	Pour information

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	19/03/2026	CJUE – 19 mars 2026 – Brillen Rottler – C-526/24 – Notion de demande abusive	La CJUE admet qu'une première demande d'accès peut, dans certaines circonstances, être qualifiées « d'excessive » et donc être traitées comme abusive. C'est notamment le cas lorsque le responsable de traitement démontre que la demande n'a pas été introduite pour prendre connaissance du traitement et en vérifier la licéité, mais dans l'intention d'artificialiser les conditions d'une demande d'indemnisation ultérieure. Elle précise que le juge national apprécie donc l'abus au regard de toutes les circonstances, et qu'il peut tenir compte d'éléments accessibles au public montrant une stratégie répétée : multiplication de demandes d'accès suivies de demandes de réparation. La Cour rappelle aussi, sur l'indemnisation, que la personne doit prouver un dommage réel, et qu'une réparation peut être écartée si le comportement du demandeur constitue la cause déterminante du préjudice allégué.	⇨ Sécuriser la gestion des demandes d'accès : traçabilité des échanges, délais, preuves de délivrance…
LE COIN RÉGLEMENTATION	19/03/2026	EDPB-EDPS - Joint Opinion 4-2026 on the Proposal for a Cybersecurity Act 2 and the Proposal on amendments to the NIS 2 Directive - March 2026 *EDPS = European Data Protection Supervisor*	L'avis conjoint analyse les deux propositions du « paquet cybersécurité » : (i) une proposition de Cybersecurity Act 2 destinée à remplacer le Cybersecurity Act pour renforcer le rôle de l'ENISA, (agence de l'Union européenne pour la cybersécurité) relancer/accélérer la certification cybersécurité et mieux traiter les risques liés à la chaîne d'approvisionnement de fournisseurs de produits et services numériques (logiciels, cloud); (ii) une proposition d'ajustements NIS 2 visant à clarifier et simplifier la conformité des entités régulées. L'EDPB et l'EDPS soutiennent l'objectif de cybersécurité (indissociable de la sécurité des données personnelles), mais rappelle un principe directeur : certaines mesures cyber	Pour information

			peuvent-elles mêmes porter atteinte aux droits fondamentaux ; elles doivent donc rester nécessaires et proportionnées. Sur le rôle de l'ENISA dans la centralisation d'informations de cybersécurité, l'avis demande de lever les ambiguïtés : si l'ENISA doit traiter des données personnelles de manière significative, cela doit être prévu explicitement dans l'acte de base, avec les éléments essentiels et les garanties ; si l'intention est de ne traiter que des données agrégées/non personnelles, cela doit aussi être clarifié (au moins au niveau des considérants). Sur la gouvernance interne, il est recommandé d'encadrer davantage les règles que le management board de l'ENISA pourrait adopter sur la protection des données, et d'y prévoir une consultation préalable de l'EDPS. Autres points structurants : appui au guichet unique de notification (réduction de charge sans baisse de protection) ; clarification attendue entre certification cybersécurité et certification RGPD, avec des synergies possibles mais sans confusion des régimes et une consultation de l'EDPB pour certains schémas de certification touchant à la sécurité des traitements.	
LE COIN RÉGLEMENTATION	19/03/2026	EDPS - Formal comments on the draft Commission Implementing Decision on adopting measures for the application of Regulation (EU) 2018/1240 as regards accessing, amending, erasing and advance erasing of data in the ETIAS Central System and repealing Commission Implementing Decision (EU) 2021/1028	L'EDPS commente le projet de décision d'exécution de la Commission pris pour l'application du règlement (UE) 2018/1240 (ETIAS), destiné à préciser les mesures et fonctionnalités relatives à l'accès, la rectification, l'effacement et l'effacement anticipé des données dans le système central ETIAS, ainsi qu'à abroger la décision d'exécution 2021/1028. Le texte s'inscrit dans la finalisation du cadre technique d'un système qui imposera aux ressortissants d'un pays tiers exemptés de visa de demander une autorisation de voyage avant l'entrée dans l'espace Schengen.	Pour information

			Sur le fond, l'EDPS salue plusieurs améliorations par rapport aux version antérieures, notamment l'introduction d'une suppression automatique de certains fichiers « d'extraction » une fois l'évaluation des risques terminées et une clarification du mode dégradé pour les contrôles aux frontières (recours à l'European Search Portal) visant à éviter un accès direct non maîtrisé au système central. Il formule toutefois deux attentes principales : (i) renforcer les spécifications fonctionnelles destinées à faciliter l'exercice effectif des droits des personnes, en regrettant l'absence de dispositions détaillées de procédure et en invitant la Commission à réintroduire un niveau de précision comparable aux versions initiales ; (ii) étendre la suppression automatique à l'ensemble des fichiers d'extraction utilisés pendant le traitement manuel, pas uniquement à une catégorie limitée afin de mieux respecter la minimisation et la limitation de conservation.	
 LE COIN RÉGLEMENTATION	19/03/2026	EDPS - Formal comments on the draft Commission Implementing Regulation specifying the details & functionalities of the systems prohibiting products made with forced labour on the Union market	L'EDPS a commenté le projet de règlement d'exécution pris pour l'application du règlement (UE) 2024/3015 interdisant la mise sur le marché de l'Union de produits issus du travail forcé. Le projet organise, dans un format standardisé, les données et informations échangées entre la Commission et les autorités compétentes sur les enquêtes, les décisions et mesures d'exécution, via un nouveau module « Forced labour » intégré à l'outil ICSMS (système de communication en matière de surveillance du marché). L'EDPS constate que le dispositif implique des données personnelles, notamment parce que la notion de « opérateur économique » peut viser des personnes physiques. Il approuve donc la référence explicite au RGPD et au règlement EUDPR. Trois points structurent ces remarques ; (i) la fixation d'une durée de conservation de 10 ans dans le module est jugée	 Pour information

			globalement justifiée (compte tenu des procédures administratives et contentieuses), mais l'EDPS demande un ajustement rédactionnel pour sécuriser le point de départ du délai, (ii) il rappelle que la limitation de conservation doit aussi être garantie lorsque les données sont extraites d'ICSMS par la Commission ou les autorités nationales, (iii) il soutient la qualification de responsabilité conjointe Commission/autorités pour ce module et recommande que cette qualification soit rappelée dans le règlement d'exécution (f non seulement dans les considérants mais aussi dans le dispositif), avec un accord de responsabilité conjointe précisant la répartition des obligations.	
 LE COIN POUR ALLER PLUS LOIN	20/03/2026	CNIL - Les dispositifs de captation sonore couplés à la vidéoprotection	La CNIL rappelle un principe clair : une caméra de vidéoprotection ne peut pas enregistrer le son. L'interdiction vise à la fois les caméras avec micro intégré et les dispositifs qui déclenchent automatiquement un enregistrement audio en lien avec la vidéoprotection, en raison des risques élevés pour la vie privée et la liberté d'expression. Elle précise néanmoins qu'un dispositif de captation sonore peut être envisageable dans certains lieux accessibles au public (accueil, commerce, etc.), hors voie publique, à condition qu'il soit distinct de la vidéoprotection : absence d'interconnexion avec les caméras, activations manuelle et ponctuelle uniquement en cas d'agression, et usage réservé au personnel directement exposé à une menace. Même dans ce cas, la CNIL encadre strictement le dispositif : il doit rester exceptionnel, nécessaire et proportionné, ne pas conduire à une surveillance permanente du personnel et la conservation des enregistrements n'est admise qu'en cas d'incident grâce. La mise en place d'une procédure interne, une information des personnes et une formation des utilisateurs, selon les cas, les instances représentatives du personnel doivent être informées/consultées.	 ⇨ Auditer et purger tout couplage audio-vidéo et vérifier que l'existant respecte l'interdiction ⇨ SI besoin, déployer un dispositif séparé et encadré : déclenchement manuel, conservation uniquement si incident, procédure interne + information

Icônes « Quelles actions ? » by Adrien Coquet

 LE COIN DES NEWS	27/03/2026	Hébergement des données de santé : le décret du 24 mars 2026 serre l'étau sur les transferts et l'extraterritorialité	Le décret n°2026-209 du 24 mars 2026, pris en application de l'article 32 de la loi n°2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (« **SREN** »), renforce le cadre règlementaire de l'hébergement de données de santé en renforçant l'exigence de territorialité, et en durcissant les obligations de transparence et de contractualisation des hébergeurs certifiés. Il crée un article R.1111-9-1 dans le code de la santé publique (« **CSP** ») : dès lors que la prestation implique du stockage, celui-ci doit être réalisé exclusivement dans l'UE/EEE. Les transferts (y compris accès à distance), vers un pays tiers ne sont envisageables que dans le cadre du RGPD : soit décisions d'adéquation soit garanties appropriées avec droits opposables/voies de recours effectives ; dans ce second cas, le contrat d'hébergement doit mentionner l'absence d'adéquation et décrire précisément les garanties et mesures complémentaires mises en place. Le décret renforce également le contenu obligatoire du contrat HDS (article R.1111-11) : périmètre et dates du certificat, description des services, lieux d'hébergement, modalités d'exercice des droits RGPD, gestion des violations, règles d'accès et conditions de transferts éventuels, restitution et destruction des données, etc.). Les dispositions clés (article R.1111-9-1 et R.1111-11 CSP) entreront en vigueur le 26 septembre 2026.	 ⇨ Cartographier les traitements HDS et planifier la mise en conformité avant le 26/09/2026 ⇨ Mettre à jour les contrats HDS