LE COIN DU DPO
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Publications de février 2026

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN RÉGLEMENTATION	03/02/2026	Conseil d'Etat 30 janvier 2026 n°506370, Ville de Nice	Le Conseil d'Etat (« CE ») a été saisi par la commune de Nice d'un recours contre une délibération de la CNIL relative à un dispositif de traitement algorithmique d'images de vidéoprotection, intitulé « zone d'intrusion entrées des écoles ». Ce dispositif visait à détecter automatiquement, en temps réel, les véhicules stationnant irrégulièrement devant les écoles et à alerter la police municipale. La CNIL avait estimé que ce traitement n'était pas autorisé en l'état du droit. Le CE rejette la requête de la commune. Il juge que les articles du code de la sécurité intérieure, qui autorisent les systèmes de vidéoprotection sur la voie publique, ne peuvent pas être interprétés, en l'absence de texte exprès, comme autorisant des traitements algorithmiques d'analyse systématique et automatisé des images. Il ajoute qu'aucune autre disposition législative ne permet de tels traitements et précise que l'argument tiré de l'absence de qualification en « IA à haut risque » au sens du règlement 2024/1689 sur l'intelligence artificielle (« AI Act ») est sans incidence sur cette absence de base légale nationale. Le CE ferme à ce stade la possibilité pour une collective de déployer ce type de vidéosurveillance algorithmique sur la voie publique sans intervention du législateur.	 ⇨ Vérifier tout projet de vidéoprotection algorithmique sur voie publique

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	03/02/2026	CNIL – Le Commissaire à la protection de la vie privée du Canada et la CNIL ont signé une déclaration de coopération	La CNIL et le Commissaire à la protection de la vie privée du Canada ont signé, le 30 janvier 2026, une déclaration de coopération visant à renforcer leur compréhension commune des nouvelles technologies et à relever conjointement les défis en matière de protection des données personnelles. L'accord signé, en marge de la table ronde virtuelle du G7 du 10 décembre 2025, prévoit notamment : la conduite de recherches conjointes, le partage de bonnes pratiques et de stratégies de régulation, ainsi que l'organisation d'ateliers communs. Ce partenariat vise à consolider les liens institutionnels et à améliorer la protection des citoyens canadiens et français.	Pour information
LE COIN RÉGLEMENTATION	03/02/2026	CNIL – Economie de la donnée : la CNIL publie son programme de travail pour 2026-2028	La CNIL présente son programme de travail 2026-2028 en matière d'économie de la donnée. Ses priorités sont de : - Mieux comprendre les modèles économiques fondés sur les données personnelles, afin d'éclairer ses décisions et renforcer la cohérence de la régulation - Mesurer l'impact économique de ses propres actions, grâce à des études d'impact, analyses sectorielles et travaux quantitatifs - Poursuivre et élargir ses travaux sur des sujets tels que la concurrence, l'économie des sanctions, l'impact du RGPD, la valeur des données personnelles et les entrepôts de données, notamment de santé. L'objectif général est d'améliorer l'expertise économique de la CNIL et de renforcer la confiance dans l'économie numérique.	Pour information

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	05/02/2026	CNIL – Hypertrucage (« deepfake ») : comment se protéger et signaler les contenus illicites ?	Les hypertrucages (« deepfakes ») sont des contenus audio, photo ou vidéo modifiés par IA pouvant imiter l'apparence ou la voie d'une personne et porter atteinte à sa vie privée, à sa réputation ou entraîner une usurpation d'identité. Leur création ou diffusion sans consentement expose à des sanctions pénales, notamment un an d'emprisonnement et 15 000 euros d'amende pour montage illicite. Pour se protéger, la CNIL commande de limiter la diffusion d'image personnelle et de signaler tout contenu illicite aux plateformes ou via PHAROS (plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements). Elle rappelle également qu'une plainte auprès de la CNIL ne remplace pas une plainte auprès de la police ou gendarmerie.	Pour information
LE COIN RÉGLEMENTATION	05/02/2026	CNIL – Traitements de données à des fins de recherche scientifique (hors santé) : quand saisir la CNIL ?	La CNIL précise qu'une saisine préalable est obligatoire lorsqu'un projet de recherche scientifique publique (hors santé) repose sur le traitement de données sensibles et qu'aucune autre exception du RGPD n'est mobilisable. Trois conditions cumulatives doivent être réunies : - La recherche doit relever de la recherche scientifique publique au sens du Code de la recherche. - Elle doit porter sur des données sensibles. - Elle doit être justifiée par un motif d'intérêt public important. La CNIL fournit également des critères pour déterminer si un projet relève bien de la recherche publique : organisme reconnu (au sens du code de la recherche), développement des connaissances et de la recherche scientifique, valorisation des résultats pour la société, etc.	⇨ Vérifier si le projet de recherche scientifique - Traite des données sensibles

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	14/02/2026	Circulaire relative à la commande publique numérique	Cette circulaire fixe une doctrine commune pour les achats numériques de l'Etat afin d'harmoniser les pratiques et d'orienter le choix entre réutilisation, achat sur étagère et développement spécifique. Elle s'applique au périmètre du système d'information de l'Etat et aux achats du domaine « informatique et télécommunications » de la nomenclature des achats de l'Etat. Elle impose une logique de décision simple : examiner d'abord les solutions mutualisées/réutilisables disponibles dans l'administration, à défaut, privilégier, lorsqu'elles existent, des solutions privées « sur étagère », en exigeant des garanties de sécurité, et une compétitivité du coût complet, et n'envisager un développement de solution spécifique que si aucune solution standard satisfaisante ne répond au besoin (coût, délai, durabilité, adaptation, etc..). Le texte demande également d'intégrer, dans le choix de l'offre, des critères structurants prioritaires : performance métier, souveraineté numérique (dépendance /risque extraterritoriaux, solutions européennes), sécurité, coût complet de solution, disponibilité, adaptabilité, maintenance, interopérabilité et durabilité. Enfin, la circulaire réaffirme l'objectif de soutien à l'innovation et aux PME dans le respect du droit de la commande publique.	Pour information
LE COIN RÉGLEMENTATION	14/02/2026	Stratégie nationale de cybersécurité 2026-2030	La stratégie nationale 2026-2030 est présentée comme une trajectoire portée au niveau de l'Etat visant à faire de la France une nation cyber de premier rang face à une menace en hausse. Elle est structurée autour de 5 piliers (et 14 objectifs) : développement des talents, résilience nationale, entrave de la cybermenace, maitrise des fondements numériques et actions européennes/internationales. Le document insiste sur un suivi interministériel via des feuilles de route à décliner par les ministères et services concernés.	Pour information

			La stratégie combine plusieurs leviers dont notamment la montée en compétence et attractivité des métiers cyber ou encore la mobilisation de leviers judiciaires/diplomatiques/techniques contre la menace et investissements des technologies critiques. Cybyermavillance.gouv.fr met en avant, pour les usagers, une plateforme nationale de prévention, le guichet « 17cyber » pour l'accompagnement des victimes.	
LE COIN POUR ALLER PLUS LOIN	14/02/2026	Cybermalveillance.gouv – Rapport de sécurisation	Cybermalveillance a publié une fiche de référence sur le rapport de sécurité. La fiche fixe un socle minimal pour les rapports remis après une prestation de sécurisation d'un système d'information (« SI »). Elle présente le rapport comme la preuve structurée de la mission avec un objectif de traçabilité, de transparence et de compréhension homogène par le client. Là encore, il est précisé que ces attendus sont notamment mobilisés dans le cadre du label ExpertCyber. La fiche de référence couvre tout le cycle de la prestation : introduction, méthodologie, évaluation du niveau de sécurité initial, déroulé l'intervention, synthèse globale avec recommandations priorisées et plan d'action, avant une conclusion centrée sur les risques résiduels et la maintenance continue.	⇨ Vérifier le format du rapport après une prestation de sécurisation du SI.
LE COIN POUR ALLER PLUS LOIN	14/02/2026	Cybermalveillance.gouv – Rapport de remédiation	Cybermalveillance a publié une fiche de référence sur le rapport de remédiation. La fiche cadre le contenu minimal attendu d'un livrable remis après un incident cyber. Elle insiste sur la finalité du rapport : documenter ce qui a été fait pour contenir, évincer/éradiquer la menace, corriger les effets. Cette fiche est présentée comme un référentiel de qualité pour les prestataires, notamment dans la logique de labellisation ExpertCyber. La structure attendue est très opérationnelle : introduction (contexte, services impactés, etc.), synthèse, diagnostic de	⇨ Vérifier le modèle interne de rapport de remédiation

			l'indicent, analyse, puis plan d'action de remédiation priorités, complété par des actions de sécurisation. Objectif de traçabilité et compréhension partagée post incident.	
LE COIN RÉGLEMENTATION	14/02/2026	CNIL – Sanctions et mesures correctrices : la CNIL présente le bilan 2025	La CNIL dresse un bilan 2025 marqué par un volume élevé de décisions répressives et correctrices : 259 décisions au total, dont 83 sanctions, 143 mises en demeure, 31 rappels aux obligations légales et 2 avertissements ; pour un montant cumulé d'amende de près de 500 millions d'euros. Elle souligne que les principaux sujets de sanction ont été les cookies/traceurs, la vidéosurveillance des salariés et la sécurité des données. Le bilan met aussi en avant la place de la procédure simplifiée, utilisée notamment pour des manquements récurrents : sécurité insuffisante, absence de réponse à la CNIL et non-respect des droits des personnes.	⇨ Vérifier la sécurité des SI et le process de réponse rapide aux demandes de la CNIL ⇨ Vérifier la conformité des cookies et droits RGPD et vidéosurveillance des salariés
LE COIN RÉGLEMENTATION	14/02/2026	Décision de la Commission constatant le niveau de protection adéquat des données à caractère personnel assuré par le Brésil	Le 27 janvier 2026, la Commission européenne a adopté une décision d'adéquation mutuelle avec le Brésil. En conséquence, les transferts de données depuis l'UE vers le Brésil peuvent s'effectuer sans mécanisme de transfert supplémentaire, dans le périmètre de la décision.	Pour information

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	14/02/2026	EDPB-EDPS Joint opinion 2/2026 on the Proposal for a regulation as regards the simplification of the digital legislative framework (Digital Omnibus) *EDPB = European Data protection Board ou Comité européen de la protection des données* *EDPS = European Data Protection Supervisor ou Contrôleur européen de la protection des données en français*	L'EDPB et l'EDPS ont adopté, le 11 février 2026, un avis conjoint 2/2026 sur la proposition dite « Digital Omnibus » visant à simplifier une partie du cadre numérique de l'UE (RGPD, ePrivacy et autres). Leur position est nuancée : ils soutiennent l'objectifs de simplification, de cohérence et de compétitivité, mais rappellent que cette simplification ne doit pas réduire le niveau de protection des personnes. L'avis identifie des évolutions jugées utiles avec quelques ajustements, notamment sur la recherche scientifique, certaines règles de notification de violation de données et d'analyse d'impact des données personnelles (« AIPD »), ainsi que des clarifications sur des sujets liés à l'IA (intérêt légitime, traitement incident de données sensibles) et à l'article 22 RGPD (décisions automatisées). En revanche, le EDPB/EPDS expriment une opposition ferme à la modification proposée de la définition de « données personnelles », estimant qu'elle rétrécirait excessivement le champ de la protection, et refusent que la Commission puisse, par acte d'exécution, définir ce qui cesserait d'être une donnée personnelle après pseudonymisation.	 Pour information
LE COIN RÉGLEMENTATION	14/02/2026	EDPB Work Programme 2026-2027	L'EDPB a adopté son programme de travail 2026-2027, le 11 février 2026, comme deuxième programme de mise en œuvre de sa stratégie 2024-2027. Le document est structuré en 4 piliers : harmonisation et conformité, culture commune de l'application de la loi et coopération, articulation avec les autres régulations numériques et dimension internationale/transferts. Il annonce notamment des travaux sur l'anonymisation, la pseudonymisation, l'intérêt légitime, les modèles « consent or pay », les données des enfants, l'IA générative, ainsi que la production de modèles UE et un cadre d'action coordonné 2026 centré sur la transparence (articles 12 à 14 RGPD).	 Pour information

LE COIN DU DPO
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	14/02/2026	EDPB - Opinion 1-2026 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of the Heineken Group	L'EDPB s'est prononcé sur un projet de décision de règles d'entreprises contraignantes (« BCR ») de responsable de traitement pour le groupe Heineken, soumis par l'autorité de protection des données néerlandaise, en tant qu'autorité chef de file. L'EDPB a conclu que le projet de BCR soumis contenait tous les éléments requis en vertu du RGPD.	Pour information
LE COIN RÉGLEMENTATION	29/01/2026	EDPB - Opinion 2-2026 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of the AkzoNobel Group	L'EDPB s'est prononcé sur un projet de décision de BCR de responsables de traitement pour le groupe AkzoNobel, soumis par l'autorité de protection des données néerlandaises, en tant qu'autorité chef de file. Le groupe AkzoNobel est une multinationale néerlandaise spécialisée dans les peintures et revêtements pour les consommateurs et les industries ainsi que dans certaines familles de produits chimiques spécialisés. L'EDPB a conclu que le projet de BCR soumis contenait tous les éléments requis en vertu du RGPD.	Pour information
LE COIN RÉGLEMENTATION	29/01/2026	EDPB - Opinion 3-2026 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of the FrieslandCampina Group	L'EDPB s'est prononcé sur un projet de décision de BCR de responsables de traitement pour le groupe FrieslandCampina, soumis par l'autorité de protection des données néerlandaises, en tant qu'autorité chef de file. Le groupe Royal FrieslandCampina est une coopérative laitière internationale basée aux Pays-Bas, née de la fusion entre Friesland Foods et Campina en 2008. Elle figure parmi les plus grandes entreprises mondiales du secteur laitier. L'EDPB a conclu que le projet de BCR soumis contenait tous les éléments requis en vertu du RGPD.	Pour information
LE COIN RÉGLEMENTATION	05/12/2025	EDPB - Opinion 4-2026 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of the ABB Group	L'EDPB s'est prononcé sur un projet de décision de BCR de responsables de traitement pour le groupe ABB (Asea Brown Boveri), soumis par l'autorité de protection des données néerlandaises, en tant qu'autorité chef de file. Le groupe ABB est une multinationale technologique spécialisée dans l'électrification, l'automatisation et la digitalisation des industries.	Pour information

			L'EDPB a conclu que le projet de BCR soumis contenait tous les éléments requis en vertu du RGPD.	
LE COIN RÉGLEMENTATION	17/02/2026	CJUE, 10 février 2026, C-97/23 P, WhatsApp Ireland c/ CEPD : un tournant procédural majeur en matière de RGPD	La CJUE juge recevable le recours de WhatsApp contre la décision contraignante 1/2021 de l'EDPB : elle considère que cette décision est un acte attaquable de l'UE et qu'elle concerne directement WhatsApp, car elle lie les autorités de contrôle (notamment irlandaise) sans marge d'appréciation sur certains constats et mesures. La Cour annule donc l'ordonnance du tribunal (qui l'avait déclaré irrecevable) et renvoie l'affaire au fond.	Pour information
LE COIN RÉGLEMENTATION	18/02/2026	Conseil d'Etat, 13 février 2026, n°498628, GERS-CEGEDIM	Le Conseil d'Etat (« CE ») rejette les recours des sociétés Gers et CEGEDIM et déclare conforme l'approche de la CNIL sur des traitements de données de santé. Le CE rappelle qu'une donnée pseudonymisée n'est pas automatiquement anonyme : elle ne peut être tenue pour anonymisée que si le risque d'identification est insignifiant et l'identification irréalisable en pratique, dans la ligne de la CJUE. Le CE a retenu que les jeux de données (âge, sexe, pathologies, prescription, dates/heures, éléments permettant d'identifier des professionnels de santé, etc.) permettraient une réidentification avec des moyens raisonnables, donc restaient des données personnelles. Le CE valide également les manquements retenus, dont l'article 66 de la loi informatique et libertés (« LIL »), et pour CEGEDIM, un manquement de licéité/transparence lié à la collecte de données via le logiciel Hri, utilisé par les médecins.	⇨ Vérifier les données de santé considérées comme « anonymisées » si la réidentification reste plausible
LE COIN RÉGLEMENTATION	19/02/2026	CNIL – Droit à l'effacement : bilan des contrôles de la CNIL dans le cadre de l'action coordonnée européenne	La CNIL indique avoir mené, en 2025, dans le cadre du plan d'action coordonné de l'EDPB, des contrôles sur place auprès de six organismes sur le droit à l'effacement. Son constat est globalement positif mais des difficultés persistent : procédures internes insuffisantes, information incomplète des personnes, difficulté à fixer les durées de conservation et à supprimer les données des sauvegardes, et	⇨ Vérifier la gestion du droit à l'effacement

			arbitrage parfois délicat entre effacement et autres droits/et libertés. La CNIL relève aussi des écarts selon la taille/secteur, puis précise avoir déjà prononcé deux mises en demeure, les autres contrôles restant en cours avec des mesures correctrices ou sanctions possibles.	
LE COIN RÉGLEMENTATION	19/02/2026	EDPB – Implementation of the right to erasure by controllers' report	L'EDPB a adopté le rapport de l'action coordonnée 2025 sur la mise en œuvre du droit à l'effacement. Ce rapport agrège les constats des autorités de contrôle européennes sur les pratiques des responsables de traitement et vise à harmoniser l'approche de contrôle et de recommandations. L'action a mobilisé 32 autorités : 9 ont engagé ou poursuivi des investigations formelles et 23 ont mené des démarches de collecte d'informations. Au total, 764 responsables de traitement ont répondu au questionnaire commun, ce qui donne au rapport une base empirique large (secteurs public et privé, tailles variées). Le rapport conclut à un niveau de conformité global plutôt « moyen », tout en identifiant des bonnes pratiques. Il met surtout en évidence 7 difficultés récurrentes : absence de procédure interne documentée, formation insuffisante, information insuffisante des personnes, mauvaise application sur les exceptions au droit à l'effacement, difficultés sur les durées de conservation, suppression dans les sauvegardes et usage inadapté de l'anonymisation comme substitut à l'effacement. Le CEPD rappelle que de nombreux modèles et guides existent déjà au niveau national, et annonce des suites possibles : renforcement de la sensibilisation, diffusion de guidance plus pratique (cas d'usage, exemples). Le rapport précise bien qu'il ne s'agisse qu'un état des lieux, certaines procédures nationales étant encore en cours.	⇨ Vérifier la gestion du droit à l'effacement

LE COIN POUR ALLER PLUS LOIN	19/02/2026	ENISA – The ENISA Cybersecurity Exercise Methodology	L'ENISA publie une méthodologie opérationnelle pour concevoir, conduire et évaluer des exercices de cybersécurité, avec un kit de support destiné à faciliter la mise en œuvre par les organisations. Le document est positionné comme un cadre commun structuré et adaptable, notamment pour les autorités publiques/acteurs institutionnels. La méthode repose sur des principes directeurs et sur une logique de jalons entre les phases, afin de sécuriser le passage d'une étape à l'autre. Elle est également présentée comme compatible avec des standards de gestions crise/exercice (ISO 22398, ISO 22361). Le cycle couvre 6 phases : initiation, conception, préparation, exécution, évaluation, puis capitalisation (« moving forward »). La méthodologie insiste sur la clarification du « pourquoi » de l'exercice, le choix du type d'exercice, la construction du scénario et de la liste maîtresse des événements à simuler (MSEL - master scenario event list), l'évaluation formalisée des résultats, puis la production d'un rapport après l'exercice et l'élaboration d'un plan d'actions avec suivi pour progresser. L'intérêt pratique du document est de standardiser la gouvernance des exercices et de transformer l'exercice en outil de pilotage.	⇨ Vérifier les modalités d'exercice de cybersécurité
LE COIN POUR ALLER PLUS LOIN	19/02/2026	EDPB – Report on stakeholder event on anonymization and pseudonymization of 12 December 2025	L'EDPB a publié, le 18 février 2026, un rapport de restitution d'un atelier parties prenantes tenu le 12 décembre 2025 sur l'anonymisation et la pseudonymisation, organisé après l'arrêt EDPB c/ SRB. L'objectif affiché est de nourrir les travaux de l'EDPB sur ses lignes directrices, sans préjuger de la position finale du Comité. Le rapport est donc un état des échanges, pas une doctrine définitive. Le document repose sur une base de consultation de 115 participants et met en évidence une attente forte de lignes	Pour information

			directrices pratiques, fondées sur des cas concrets et une analyse contextuelle de l'identifiabilité. Les participants ont surtout signalé des difficultés dans les chaînes de traitement (responsable/sous-traitant, co-responsabilité, partage à des tiers), dans l'évaluation des capacités réelles de réidentification selon les destinataires, et dans l'évolution des risques dans le temps (nouveaux acteurs, croisement de données). Un point saillant du rapport est la prudence exprimée sur les données pseudonymisées : pour de nombreux cas de partage, plusieurs participants estiment qu'il faut partir du principe que les données restent personnelles pour le destinataire tant que l'anonymat n'est pas démontré et documenté. Le rapport recense aussi des leviers concrets discutés par les participants : mesures contractuelles, organisationnelles et mesure technique avec un rappel constant de la minimisation et de la suppression des données inutiles.	
LE COIN RÉGLEMENTATION	19/02/2026	EDPS – Opinion 1-2026 on the Proposal for a regulation amending Regulation (EU) No 904/2010 as regards access of the EPPO and OLAF to VAT information L'EPPO : European PP Office = Office européen de lutte antifraude OLAF : bureau européen de lutte antifraude)	L'EDPS a rendu un avis sur la proposition de règlement du Conseil visant à modifier le règlement (UE) n°904/2010 pour permettre à l'EPPO (Office européen de lutte antifraude) et à OLAF (bureau européen de lutte antifraude) d'accéder de façon ciblée et centralisée, à certaines informations TVA au niveau de l'UE afin de mieux lutter contre la fraude transfrontalière. L'EDPS soutient l'objectif et admet la nécessité » d'un accès direct limité, compte tenu du caractère transnational des fraudes et des limites du modèle actuel de coopération. L'avis insiste sur la préservation de la frontière entre traitements administratifs et traitements à des fins répressives/pénales. L'EDPS demande que le texte précise clairement le caractère exceptionnel de cet accès direct à des bases administratives, pour éviter qu'il ne serve de précédent à des applications/accès plus larges. L'EDPS recommande de mieux expliciter les catégories de données concernées, de	Pour information

			limiter les informations transmises par Eurofisc au strict nécessaire pour décider de l'ouverture d'une enquête et d'inscrire dans le règlement de base des garde-fous. Parmi les garanties demandées figurent notamment : des restrictions techniques sur les résultats, une traçabilité complète de chaque accès (utilisateur identifié), journaux d'audit supervisés, possibilité pour les autorités nationales d'être informées et de contester un accès excessif, ainsi qu'un suivi spécifique lors des futures évaluations du dispositif.	
LE COIN RÉGLEMENTATION	19/02/2026	EDPS – Opinion 2-2026 on the Proposal for a regulation amending Directives (EU) 2026/2341 and 2016/97 as regards the strengthening of framework for occupational retirement provision	Dans son avis du 9 janvier 2026 sur la proposition de directive modifiant les directives 2016/2341et 2016/97 (renforcement du cadre de la retraite professionnelle), l'EDPS soutient l'objectif de transparence et de meilleure information des affiliés/bénéficiaires, mais alerte sur l'impact « data protection » : les données de retraite sont des données personnelles et peuvent inclure des données sensibles. L'EDPS demande donc un encadrement plus précis des traitements, en particulier pour les systèmes de suivi des pensions (portails/apps de suivi des droits), la définition des données utilisées pour évaluer la tolérance au risque des affiliés, et les contrôles « fit and proper » des dirigeants/fonctions clés des IORP (institutions de retraite professionnelle). Il recommande aussi de sécuriser les renvois explicites au RGPD et au règlement (UE) 2018/1725 (EUDPR).	Pour information
LE COIN RÉGLEMENTATION	19/02/2026	EDPS – Opinion 3-2026 on the Proposal for a Regulation amending Regulation (EU) 2019/1238 on a pan-European Personal Pension Product (PEPP) PEPP (pan-european personal pension – plan de retraite personnel paneuropéen)	L'EDPS examine la proposition de règlement modifiant le règlement (UE) 2019/1238 sur le PEPP (pan-european personnal pension – plan de retraite personnel paneuropéen), adoptée par la Commission le 20 novembre 2025. L'objectif du texte est de rendre le PEPP plus opérationnel et attractif afin de compléter les régimes de retraite nationaux et professionnels. L'EDPS accueille favorablement cet objectif, en particulier la portabilité et la transparence du produit.	Pour information

			L'EDPS rappelle toutefois que les données des épargnants et bénéficiaires PEPP sont des données personnelles et que certains contrats PEPP peuvent impliquer des données sensibles (notamment de santé). Il insiste donc sur la nécessité de définir clairement les catégories de données collectées/partagées et les garanties applicables. Ses recommandations principales portent sur quatre points ; ajouter une référence au règlement 2018/1725 (EUDPR) en plus du RGPD dans le considérant pertinent, clarifier si les PEPP impliquent du profilage au sens du RGPD, définir les catégories de données transmises et leur traitement ultérieur, idéalement via des règes plus précises (actes d'exécution ou acte délégué).	
LE COIN RÉGLEMENTATION	19/02/2026	EDPS – Opinion 4-2026 on the Proposal for a Regulation amending Regulation establishing a framework of measures to facilitate the transport of military equipment, goods and personal across the Union	L'EDPS examine la proposition de règlement créant un cadre européen pour faciliter le transport de matériels, biens et personnels militaires à travers l'UE (« military mobility »). L'EDPS soutient l'objectif général (capacité de réaction aux crises, sécurité/défense, etc.) et relève que le futur dispositif implique des échanges d'informations contenant potentiellement des données personnelles. Sur le volet « protection des données », l'EDPS accueille favorablement les références explicites au RGPD, au règlement 2018/1725 (EUDR) et à la directive ePrivacy, ainsi que les règles de confidentialité/sécurité et la limitation de la finalité (usage des informations uniquement pour l'objectif demandé). Son point de vigilance principal porte sur les futurs systèmes d'échange d'information : l'EDPS demande que les actes d'exécution précisent clairement les catégories de données traitées, les durées de conservation et les rôles/responsabilités des responsables de traitements, et rappelle qu'il devra être consulté sur ces actes.	Pour information

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	19/02/2026	EDPS – Opinion 5-2026 on the Proposal for a Regulation on the establishment of European Business Wallets	. L'EDPS examine la proposition de règlement instituant des European Business Wallets (portefeuilles numériques pour les échanges B2B/B2G) et un European Digital Directory destiné à rendre ces portefeuilles « découvrables » et interopérables à l'échelle de l'UE. Il soutient l'objectif de confiance et de fluidification des échanges, mais rappelle que, même si l'outil vise des opérateurs économiques, il implique nécessairement des données personnelles. L'EDPS formule deux demandes principales : (i) ne pas cantonner les garanties « protection des données » au seul annuaire, mais les poser comme un principe transversal applicable à l'ensemble du dispositif, en rappelant aussi l'applicabilité du règlement (UE) 2018/1725 lorsque des institutions de l'UE (notamment la Commission) traite des données ; (ii) renforcer la gouvernance de supervision en prévoyant explicitement une coopération Commission- EDPS lors que la Commission agit comme autorité de contrôle pour des entités de l'UE fournissant des Business Wallets.	Pour information
LE COIN RÉGLEMENTATION	19/02/2026	EDPS – Opinion 6-2026 on the Proposal for a Regulation as regards the further development of capital market integration and supervision within the Union	L'EDPS examine la proposition de règlement de la Commission (COM (2025) 943) visant à renforcer l'intégration des marchés capitaux et à centraliser davantage certaines fonctions de supervision au niveau de l'UE, notamment autour de l'ESMA (autorité européenne des marchés financiers). L'EDPS soutient l'objectif général de simplification, tout en rappelant que cette logique doit rester compatible avec une protection robuste des données des personnes concernées. L'avis est globalement favorable, mais il formule plusieurs demandes de clarifications importantes. D'abord, sur les transferts internationaux, l'EDPS demande de préciser explicitement que l'ESMA applique le règlement 2018/1725 (EUDPR) lorsqu'elle transfère des données personnelles via	Pour information

			des accords/arrangements administratifs avec des autotriés de pays tiers, et rappelle qu'une autorisation préalable de l'EDPS est requise dans certains cas. Ensuite, sur la future plateforme de données opérées par l'ESMA, il souligne une certaine ambiguïté sur les rôles (RT/ST) et recommande de clarifier les responsabilités de l'ESMA et des entités qui soumettent ou consultent les données. L'EDPS attire également l'attention sur l'ESAP (European Single Access Point) : les données transmises ne doivent contenir des données personnelles que si cela est requis par le droit applicable ou strictement nécessaire, et ces obligations devraient être rappelées plus clairement dans le texte.	
LE COIN RÉGLEMENTATION	19/02/2026	EDPS – Opinion 7-2026 on the Proposal for a Regulation extending the application of Regulation (EU) 2021/1232	L'EDPS s'est prononcé sur la proposition de règlement prolongeant la durée d'application du règlement (UE) 2021/1232 (régime transitoire permettant certaines dérogations ePrivacy pour la détection volontaire de contenus pédocriminels en ligne), afin d'éviter une rupture juridique avant l'adoption du cadre pérenne. La proposition vise à prolonger ce régime jusqu'au 3 avril 2028. L'EDPS reconnaît la gravité des infractions visées et la légitimité de l'objectif de luette contre les abus sexuels sur mineurs. Son avis est toutefois très conditionné sur le plan des garanties. L'EDPS considère que cette prolongation est justement l'occasion de corriger deux faiblesses structurelles du régime transitoire : l'absence de base légale suffisamment claire au regard du RGPD et l'insuffisance de garanties contre des formes de surveillance généralisée et indifférenciée. Il recommande d'inscrire une base légale explicite pour certains traitements et de mieux encadrer la licéité des traitements dans le texte lui-même. L'EDPS insiste aussi sur la nécessité de préciser quelles catégories de données peuvent être traitées pour quelles	Pour information

			finalités et de prendre en compte les risques propres aux technologies de détection.	
LE COIN RÉGLEMENTATION	21/02/2026	EDPS – Formal comments on draft Commission Delegated Regulation amending Regulation (EU) 2018/858 as regards the standardized access to vehicle on-board diagnostics information and repair and maintenance information, and the requirements and procedures for secure access to on-board diagnostic information	L'EDPS a publié, le 20 février 2026, des commentaires formels sur le projet de règlement délégué de la Commission modifiant le règlement (UE) 2018/858, relatif à l'accès standardisé aux informations de diagnostic embarqué et de réparation /maintenance ainsi qu'aux conditions d'accès sécurisé à ces informations. Le texte vise surtout à mettre à jour les exigences techniques d'accès (via l'annexe X du règlement de base), dans un contexte de cybersécurité et d'évolution technique. Sur le plan « protection des données », l'EDPS relève que le dispositif peut impliquer des données personnelles (notamment via le VIN permettant d'identifier un véhicule, et des informations relatives aux employés des opérateurs accédant aux données OBD). Il accueille favorablement la référence au RGPD dans le projet mais recommande de formuler plus largement le considérant concerné pour viser l'applicabilité du RGPD et la directive ePrivacy dans l'exécution du futur règlement. Hormis ce point, l'EDPS estime que les modifications proposées ne soulèvent pas de difficulté spécifique supplémentaire du point de vue de la protection des données.	Pour information
LE COIN RÉGLEMENTATION	27/02/2026	Projet de recommandation concernant les outils de rejeu de session	La CNIL a ouvert une consultation publique jusqu'au 22 avril 2026 sur un projet de recommandation visant à encadrer les outils de rejeu de session (souvent utilisés pour reconstituer la navigation et analyser les difficultés rencontrées sur un site/une app). L'objectif est double : clarifier les exigences applicables aux éditeurs (responsables de traitement) et fixer des attentes concrètes pour les fournisseurs (sous-traitants), afin que ces solutions soient configurables et déployables de manière conforme. Le projet insiste sur la logique « privacy by design/by default » : la configuration doit permettre de respecter minimisation,	Pour information

			durée de conservation et sécurité. Il recommande notamment de limiter le nombre de sessions collectées, d'activer un masquage robuste et de réduire la ré-identification via des identifiants moins corrélables. Le texte demande aussi que la solution permette de paramétrer les durées et de supprimer des sessions individuelles (y compris pour répondre aux demandes d'effacement), et prévoir des exigences de sécurité (ex. gestion des habilitations ou encore blocage de collecte de données très sensibles).	
 LE COIN POUR ALLER PLUS LOIN	27/02/2026	Joint statement on AI- Generated Imagery and the Protection of Privacy	Une déclaration conjointe coordonnée au sein de la Global Privacy Assembly rassemble 61 autorités pour alerter sur les risques liés aux IA capables de générer des images/vidéos réalistes représentant des personnes identifiables sans qu'elles ne le sachent ni y consentent. Le texte met en avant les préjudices possibles tels que l'atteinte à la dignité, les contenus intimes non consentis ou la diffamation, avec une vigilance particulière sur les enfants publics vulnérables. La déclaration formule des attentes « socle » à destination des organisations qui développent ou déploient ces systèmes : garde-fous techniques et organisationnels contre les usages abusifs, transparences sur les capacités/limites et les règles d'utilisation, mécanismes accessibles de retrait/suspension des contenus préjudiciables, et mesures renforcées spécifiques pour la protection des mineurs. Les signataires annoncent également une volonté de réponse coordonnée et invitent les acteurs à travailler proactivement avec les régulateurs.	 Pour information