LE COIN DU DPO
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Publications de Décembre 2025

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
 LE COIN RÉGLEMENTATION	03/12/2025	CNIL – La Caisse des Dépôts et la CNIL renforcent leur coopération pour accompagner l'usage responsable des données personnelles et de l'IA – 1er décembre 2025	Le 1er décembre 2025, la Caisse des Dépôts et la CNIL ont signé une convention de partenariat afin de renforcer et structurer leur coopération sur les enjeux de protection des données personnelles et d'usage responsable de l'intelligence artificielle (« IA »). Ce partenariat vise à accompagner les projets numériques de la Caisse des Dépôts dans un cadre sécurisé, conforme à la réglementation et respectueux des droits des personnes, notamment en matière de vie privée. Il s'inscrit dans la modernisation des politiques publiques, en particulier dans les domaines des politiques sociales, des retraites, de la formation professionnelle et de la lutte contre la fraude aux aides publiques. La convention prévoit : - Un accompagnement de la Caisse des Dépôts par la CNIL sur la conformité des traitements de données et des usages de l'IA ; - Des actions de sensibilisation des équipes et des métiers aux enjeux de protection des données, en particulier pour les données sensibles ; - Une contribution de la Caisse des Dépôts aux travaux de la CNIL ; - La réalisation de travaux communs, notamment sur l'impact des évolutions réglementaires. Un comité de pilotage annuel assurera le suivi des actions et l'identification de nouveaux axes de collaboration.	 Pour information

			L'objectif commun est de promouvoir un numérique responsable, conciliant innovation, intelligence artificielle et respect des droits fondamentaux des citoyens.	
LE COIN RÉGLEMENTATION	03/12/2025	Délibération n°SAN-2025-011 du 27 novembre 2025 concernant la société AMERICAN EXPRESS CARTE FRANCE	Le 27 novembre 2025, la CNIL a infligé une amende de 1,5 million d'euros à la société AMERICAN EXPRESS CARTE FRANCE, filiale française du groupe American Express, pour non-respect des règles relatives aux cookies et autres traceurs prévues par l'article 82 de la loi Informatique et Libertés. À la suite de contrôles réalisés en janvier 2023 sur le site americanexpress.com/fr-fr et dans les locaux de la société, la CNIL a constaté plusieurs manquements graves au recueil et au respect du consentement des internautes : - Dépôt de traceurs sans consentement, dès l'arrivée de l'utilisateur sur le site, avant toute action de sa part, y compris des cookies à finalité publicitaire ; - Dépôt de traceurs malgré le refus explicite de l'utilisateur ; - Lecture de traceurs après le retrait du consentement, alors que ceux-ci auraient dû cesser d'être utilisés. Le montant de la sanction tient compte du caractère multiple et répété des manquements, du fait que les règles applicables aux cookies sont anciennes, bien établies et largement diffusées par la CNIL, mais aussi de la mise en conformité de la société au cours de la procédure, retenue comme circonstance atténuante.	⇨ En de recours à des cookies, s'assurer de leur nature et de bien respecter les règles applicables au consentement s'il est requis.

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	05/12/2025	EDPB – Recommendations 2-2025 on the legal basis for requiring the creation of user accounts on e-commerce websites – December 2025 *EDPB = European Data protection Board ou Comité européen de la protection des données*	L'EDPB analyse la pratique courante des sites de commerce en ligne consistant à imposer la création d'un compte utilisateur pour accéder aux offres ou effectuer des achats. Si cette exigence est souvent justifiée par des raisons commerciales ou organisationnelles telles que la gestion des commandes, l'accès à des services ou offres spécifiques, l'EDPB souligne qu'elle expose les personnes concernées à des risques supplémentaires pour leurs droits et libertés, notamment en matière de protection des données personnelles. L'EDPB formule des recommandations afin de déterminer les conditions de création obligatoire d'un compte licite au regard du RGPD, en particulier au titre : - De l'exécution d'un contrat (article 6.1.b)), - D'une obligation légale (article 6.1.c)), ou - De l'intérêt légitime du responsable de traitement (article 6.1.f)). À l'issue de l'analyse de plusieurs cas d'usage, l'EDPB conclut que l'imposition de la création d'un compte ne peut être justifiée que dans un nombre très limité de situations, par exemple pour la fourniture d'un service par abonnement ou l'accès à des offres exclusives. En revanche, dans la majorité des cas examinés, cette obligation ne satisfait pas aux conditions de licéité du RGPD, car la création d'un compte n'est pas nécessaire pour atteindre les finalités poursuivies. L'EDPB estime donc que proposer une alternative « achat en tant qu'invité » constitue généralement la solution la plus appropriée. Ce mode permet de limiter la collecte de données personnelles, respecte davantage les principes de minimisation des données, de transparence. Il s'inscrit dans	⇨ En de site marchand, s'assurer de la nécessité d'imposer la création d'un compte client

			l'obligation de protection des données dès la conception et par défaut prévue à l'article 25 du RGPD.	
LE COIN RÉGLEMENTATION	05/12/2025	EDPS – High-Risk AI Systems Mapping Report in European Institutions, Agencies and Bodies – December 2025 *EDPS = European Data Protection Supervisor* *ou Contrôleur européen de la protection des données en français*	L'EDPS a publié un rapport de cartographie des systèmes d'IA à haut risque utilisés par les institutions, agences et organes de l'Union européenne. Ce rapport, l'un des premiers exercices de ce type réalisés par une autorité de surveillance dans le cadre de l'AI Act, met en lumière une difficulté majeure et largement partagée : les organisations peinent à identifier précisément les systèmes d'IA qu'elles utilisent réellement. Le rapport montre que le principal obstacle ne réside pas uniquement dans la qualification d'un système comme « à haut risque », mais d'abord dans sa découverte. Les méthodes traditionnelles d'inventaire informatique supposent une maîtrise centralisée des outils, alors que l'IA se diffuse de manière décentralisée, souvent sans validation formelle par l'IT ou les équipes conformité. Le rapport souligne également les limites des approches fondées sur la déclaration volontaire des usages par les départements. Les utilisateurs métiers ne disposent pas toujours des compétences nécessaires pour identifier ce qui constitue juridiquement un système d'IA, et les outils testés en pilote ou adoptés de manière informelle restent largement invisibles. À cela s'ajoutent la complexité organisationnelle et la vitesse d'adoption des nouvelles solutions, qui rendent rapidement obsolètes les inventaires statiques. En conclusion, le rapport de l'EDPS met en évidence que les méthodes classiques de recensement des outils sont inadaptées à l'ère de l'IA. Pour se conformer efficacement au AI Act, les organisations doivent repenser leurs	Pour information

			stratégies de découverte et de gouvernance des usages de l'IA, afin d'identifier en continu des systèmes diffus, évolutifs et souvent non déclarés.	
LE COIN RÉGLEMENTATION	08/12/2025	Délibération n°HAB-2025-006 du 27 novembre 2025 habilitant des agents de la Commission nationale de l'informatique et des libertés à procéder à des missions de vérification	La liste des agents de la CNIL habilités à établir effectuer des visites et vérifications a été mise à jour par la CNIL.	Pour information
LE COIN RÉGLEMENTATION	12/12/2025	Règlement (UE) 2025/2518 du Parlement européen et du Conseil du 26 novembre 2025 établissant des règles de procédure supplémentaires relatives à l'application du règlement (UE) 2016/679	Le règlement (UE) 2025/2518, publié en décembre 2025, crée un cadre européen harmonisé pour faciliter le traitement des affaires transfrontalières en protection des données. Il simplifie et accélère la coopération entre autorités nationales, clarifie les règles sur les plaintes et renforce les droits des parties. Ce règlement fixe des délais indicatifs, introduit des procédures adaptées selon la complexité des dossiers, et améliore la transparence grâce à un outil numérique commun et un rôle renforcé de l'EDPB. Un délai de 15 mois avant application garantit la sécurité juridique.	Pour information
LE COIN RÉGLEMENTATION	18/12/2025	CNIL – Prospection politique : la CNIL sanctionne cinq candidats aux élections européennes et législatives 2024 – Décembre 2025	En décembre 2025, la CNIL a sanctionné cinq candidats aux élections européennes et législatives de 2024 pour des violations des règles de protection des données dans l'envoi de messages de prospection politique. Ces sanctions, prononcées via une procédure simplifiée, totalisent 23 500 euros. Les manquements constatés sont multiples : - Incapacité à justifier la licéité du traitement (article 5.2 RGPD) : les candidats n'ont pas pu prouver le consentement des destinataires ou démontrer que leur intérêt légitime justifiait l'envoi des messages ;	⇨ Quel que soit le traitement mis en place, s'assurer de : - La licéité du traitement ; - La sécurité et confidentialité des données ;

			- Utilisation des données à des fins incompatibles (article 5.1.b) RGPD) : un candidat professionnel de santé a utilisé les données de ses patients recueillies pour des soins afin de faire de la prospection politique, ce qui est prohibé ; - Défaut d'information des personnes concernées (articles 12, 13, 14 RGPD) : les messages envoyés ne comportaient pas ou partiellement les informations légales requises ; - Absence de dispositif facilitant le droit d'opposition (articles 12 et 21 RGPD) : deux candidats n'avaient pas mis en place de moyen simple pour que les destinataires refusent de recevoir d'autres messages (comme un lien ou un SMS STOP) ; - Manquement à répondre aux demandes d'exercice des droits (articles 12, 15, 17 RGPD) : un candidat a ignoré une demande d'accès et d'effacement des données. La CNIL lui a adressé une injonction pour y répondre ; - Défaut de confidentialité des données (article 32 RGPD) : un candidat a envoyé un mail à plusieurs centaines de personnes en divulguant leurs adresses électroniques visibles, portant atteinte à la confidentialité, particulièrement grave vu la nature sensible des données politiques. Ces sanctions rappellent que les candidats restent pleinement responsables de la conformité de leurs traitements, même lorsqu'ils font appel à des prestataires externes pour la prospection politique.	- L'information des personnes ; - L'exercice des droits des personnes concernées.

Icônes « Quelles actions ? » by Adrien Coquet

 LE COIN POUR ALLER PLUS LOIN	18/12/2025	CNIL – La CNIL publie un outil pour la traçabilité des modèles d'IA publiés en source ouverte – Décembre 2025	La CNIL a publié un outil de démonstration permettant de naviguer dans la généalogie des modèles d'IA publiés en open source. Cet outil facilite la traçabilité des modèles, essentielle pour comprendre leur constitution et aider à l'exercice des droits des personnes concernées (opposition, accès, effacement). La publication de modèles open source permet une large diffusion, avec des utilisateurs qui modifient et republient ces modèles, créant ainsi un réseau d'ascendants et descendants. Comprendre cette généalogie est crucial, notamment parce que les modèles d'IA générative peuvent mémoriser des données personnelles extraites de leurs bases d'entraînement. La CNIL rappelle que, dans la plupart des cas, ces modèles sont soumis au RGPD, sauf si le responsable du traitement démontre que les données personnelles ne peuvent être extraites. L'outil développé en collaboration avec le Laboratoire d'Innovation Numérique (« LINC ») aide à explorer ces relations entre modèles sur la plateforme HuggingFace, ouvrant la voie à une meilleure transparence et responsabilisation dans le traitement des données personnelles par les IA open source.	 Pour information
 LE COIN RÉGLEMENTATION	18/12/2025	EDPS – Formal comments on the draft Commission Implementing Regulation laying down provisions on electronic licences for the export of cultural goods under Council Regulation (EC) No 116/2009 and repealing Commission Implementing Regulation (EU)No 1081/2012 – December 2025	L'EDPS a été consulté par la Commission européenne sur le projet de règlement d'exécution concernant les réactions aux violations de sécurité des portefeuilles d'identité numérique européens (EUDIWs). Le projet de règlement d'exécution vise à définir des règles pour réagir aux incidents de sécurité des portefeuilles numériques, en cohérence avec les normes techniques et les recommandations de la Commission.	 Pour information

			L'EDPS souligne que le RGPD et la directive ePrivacy s'appliquent aux traitements de données personnelles liés aux portefeuilles numériques. Il recommande également de rappeler que le Règlement (UE) 2018/1725 (« EUDPR ») s'applique si la Commission traite des données personnelles dans ce cadre. S'agissant de la notification des violations de sécurité, les Etats membres doivent informer rapidement les autorités de protection des données en plus de notifier la Commission et les points de contact nationaux. L'EDPS insiste sur la nécessité de définir clairement les informations minimales à communiquer aux utilisateurs affectés et aux tiers concernés en cas de suspension ou de retrait d'un portefeuille. Les notifications doivent inclure les mesures que les utilisateurs peuvent prendre pour limiter les impacts de la violation et les coordonnées des fournisseurs de la solution de portefeuille. Aussi, l'EDPS recommande d'élargir les critères de gravité pour inclure toutes les données personnelles susceptibles d'affecter négativement les personnes concernées, pas seulement les catégories sensibles, par exemple les données de cartes bancaires.	
LE COIN RÉGLEMENTATION	19/12/2025	Délibération n° SAN-2025-014 du 11 décembre 2025 concernant la société MOBIUS SOLUTIONS LTD	Le 11 décembre 2025, la CNIL a sanctionné MOBIUS SOLUTIONS LTD, ancien sous-traitant de DEEZER, d'une amende d'un million d'euros pour manquements au RGPD dans le cadre d'une violation de données touchant plus de 46 millions d'utilisateurs. En novembre 2022, DEEZER a signalé que des données d'utilisateurs avaient été mises en ligne sur le darknet,	⇨ Un registre de traitement doit être mis en place pour les activités pour lesquelles

			impliquant MOBIUS SOLUTIONS LTD. La CNIL a contrôlé la société en 2023-2024 et constaté plusieurs infractions : - Non-suppression des données après la fin du contrat (article 28.3.g) RGPD) : la société a conservé illégalement les données de DEEZER ; - Non-respect des instructions du responsable de traitement (article 29 RGPD) : les données ont été utilisées pour améliorer ses propres services, sans autorisation ; - Absence de registre des activités de traitement (article 30 RGPD) : MOBIUS SOLUTIONS LTD n'a pas tenu de registre obligatoire en tant que sous-traitant. Même si la société MOBIUS SOLUTIONS LTD est hors UE, la CNIL reste compétente pour la sanctionner car les traitements ont concerné des utilisateurs français et constituaient un suivi du comportement des personnes sur le territoire français.	l'organisme est sous-traitant et un pour lesquelles l'organisme est responsable de traitement. ⇨ Le contrat entre le responsable de traitement et le sous-traitant doit reprendre l'ensemble des exigences de l'article 28 RGPD et doit être respecté !
LE COIN RÉGLEMENTATION	19/12/2025	EDPS - Opinion 30-2025 on the signing and conclusion of an Agreement between the EU and the Swiss Confederation on the transfer of Passenger Name Record data - December 2025	La Commission européenne a consulté l'EDPS sur deux propositions d'accords permettant le transfert de données de réservation de passagers (PNR) vers la Suisse pour lutter contre le terrorisme et la criminalité grave. L'EDPS rappelle que le transfert de ces données constitue une atteinte aux droits fondamentaux à la vie privée et à la protection des données, et doit respecter la législation de l'UE, notamment le RGPD, la Directive PNR et la Directive sur la protection des données dans la justice pénale. L'EDPS insiste sur le fait que tout transfert de données PNR doit être nécessaire, proportionné et encadré par des garanties strictes, conformément à la jurisprudence de la Cour de justice de l'Union européenne et aux standards	Pour information

			internationaux (ONU, Organisation de l'aviation civile internationale « OACI »). L'EDPS note que l'accord interdit le traitement de catégories spéciales de PNR, aligné sur la définition du RGPD et de la LED (loi de protection des données suisse). L'EDPS souligne que l'accord prévoit des mécanismes pour suspendre ou mettre fin à l'accord en cas de non-respect sérieux et persistant. Il relève que la Suisse peut utiliser le routeur technique commun pour le transfert des données, sous conditions établies par la réglementation européenne. Enfin, l'EDPS insiste que la Suisse ne peut partager les données traitées qu'avec Europol ou Eurojust uniquement dans le cadre de leurs mandats respectifs et selon les règles de la Directive PNR, pour éviter des transferts qui ne seraient pas permis au sein de l'Union européenne. L'EDPS estime que le projet d'accord contient les garanties nécessaires pour être compatible avec le cadre juridique européen en matière de protection des données personnelles.	
LE COIN RÉGLEMENTATION	19/12/2025	EDPS - Formal comments on the draft Commission Delegated Regulation amending Regulation (EU) 2018/1862 of the European Parliament and of the Council as regards the sub-categories of objects of high value in the Schengen Information System - December 2025	L'EDPS a été consulté par la Commission européenne sur le projet de règlement délégué modifiant le règlement (UE) 2018/1862 concernant les sous-catégories d'objets de grande valeur dans le Système d'Information Schengen (SIS). Le SIS-Police est utilisé pour la coopération policière et judiciaire, notamment pour les alertes sur les objets à saisir ou à utiliser comme preuves.	Pour information

			Le projet de règlement délégué vise à introduire de nouvelles sous-catégories d'objets de grande valeur dans le SIS, comme les vélos électriques, montres connectées, appareils médicaux portables. L'EDPS relève que certaines de ces nouvelles catégories d'objets sont des objets connectés ou « smart » pouvant contenir des données personnelles, y compris des données sensibles. L'EDPS rappelle que l'accès et l'extraction de données à partir de ces objets pour les besoins d'enquêtes ou de procédures judiciaires doit respecter le cadre légal européen sur la protection des données, tel que prévu dans le règlement SIS. Pour le reste, l'EDPS n'a pas d'autres commentaires ou recommandations sur le projet.	