LE COIN DU DPO
veille pour vous

Icônes « Quelles actions ? » by Adrien Coquet

Publications de Octobre 2025

Quel coin ?	Date de publication	Document	Que retenir ?	Quelles actions ?
LE COIN RÉGLEMENTATION	02/10/2025	Délibération n°HABS-2025-005 du 25 septembre 2025 habilitant des agents de la Commission nationale de l'informatique et des libertés à établir un rapport en application du cinquième alinéa de l'article 22-1 de la loi n° 78-17 du 6 janvier 1978 modifiée	La liste des agents de la direction des contrôles et des sanctions de la CNIL, habilités à établir un rapport dans le cadre de la procédure simplifiée a été mise à jour par la CNIL.	Pour information
LE COIN RÉGLEMENTATION	02/10/2025	CNIL – La CNIL et Inria renforcent leur partenariat pour la protection des données personnelles et l'évaluation des algorithmes – Octobre 2025	La CNIL et l'Institut national de recherche en sciences et technologies du numérique (« Inria ») ont signé une nouvelle convention de partenariat afin de renforcer leurs travaux communs sur la protection des données, la vie privée et l'évaluation des algorithmes et des systèmes d'intelligence artificielle (« IA »). Ce renouvellement prolonge plus de dix ans de coopération entre les deux institutions, dans un contexte marqué par la mise en œuvre du RGPD et du règlement européen sur l'intelligence artificielle (« AI Act »). Ce partenariat illustre une volonté commune de concilier innovation technologique et protection des droits fondamentaux. La CNIL et l'Inria affirment que le développement de l'IA doit intégrer dès sa conception les principes de transparence, d'éthique et de respect de la vie privée, afin d'assurer une innovation durable et bénéfique pour les citoyens européens.	Pour information

Icônes « Quelles actions ? » by Adrien Coquet

 LE COIN RÉGLEMENTATION	14/10/2025	CNIL – La CNIL prononce 16 nouvelles sanctions dans le cadre de la procédure simplifiée – Octobre 2025	Depuis mai 2025, la CNIL a prononcé seize sanctions dans le cadre de la procédure simplifiée pour un montant total de 108 000 €, dont quatorze issues de plaintes. Les manquements constatés concernent principalement la vidéosurveillance, la prospection commerciale sans consentement et le défaut de coopération avec l'autorité. S'agissant de la vidéosurveillance : - Des sanctions ont visé une société pharmaceutique, un établissement hospitalier et un établissement scolaire pour non-respect du principe de minimisation des données (article 5.1.c RGPD). - Les dispositifs filmaient des locaux syndicaux ou des élèves dans des espaces de vie, atteignant ainsi la vie privée. - L'hôpital a également été sanctionné pour détournement de finalité (article 5.1.b RGPD) après avoir transmis des images à une compagnie d'assurance. S'agissant de la prospection commerciale : - Une société a été sanctionnée pour avoir utilisé des formulaires de jeux-concours biaisés afin de collecter des données à des fins de prospection sans consentement valable, en infraction avec l'article L. 34-5 du Code des postes et des communications électroniques. S'agissant du défaut de coopération : - Dix des seize sanctions concernent des avocats, médecins ou entreprises n'ayant pas répondu aux demandes de la CNIL, en violation de l'article 18 de la loi Informatique et Libertés, qui impose aux	

			organismes de faciliter les missions de contrôle de l'autorité.	
 LE COIN DES FONDAMENTAUX	14/10/2025	CNIL – Programmes de fidélité : la CNIL précise l'application du droit à la portabilité des données – Octobre 2025	Saisie par les acteurs de la distribution, la CNIL précise les données concernées par le droit à la portabilité dans les programmes de fidélité. Sur les codes-barres des produits : Le code-barre (GTIN), associé à l'identité du client, constitue une donnée personnelle. Le client peut donc y accéder et en demander la portabilité ; le distributeur ou l'organisme mandaté doit les transmettre sur demande. Sur les montants des promotions : Le montant des réductions obtenues (différence entre le prix initial et le prix après promotion) est également une donnée portable, dès lors qu'elle peut être rattachée à un client identifiable. Sur les méthodes de calcul exclues : La CNIL considère, en revanche, que les algorithmes ou modes de calcul utilisés pour déterminer les promotions ne sont pas des données personnelles et ne relèvent pas du droit à la portabilité.	 Pour information
 LE COIN RÉGLEMENTATION	14/10/2025	EDPB-European Commission – Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation – October 2025 *EDPB = European Data protection Board ou Comité européen de la protection des données*	EN CONSULTATION jusqu'au 4 décembre 2025 Le Digital Market Act (« DMA ») et le RGPD poursuivent des objectifs distincts mais complémentaires : - Le RGPD protège les personnes physiques face au traitement de leurs données personnelles, - Le DMA encadre les pratiques des gatekeepers (grands acteurs du numérique) afin de garantir des marchés numériques équitables et contestables en Europe.	 Pour information

			L'EDPB et la Commission européenne ont annoncé, le 10 septembre 2024, l'élaboration de lignes directrices conjointes pour assurer une application cohérente et compatible des deux textes, conformément à la jurisprudence de la Cour de justice de l'Union européenne (« CJUE »). Cette initiative s'inscrit dans la stratégie 2024-2027 de l'EDPB visant à renforcer la coopération inter-réglementaire dans le champ numérique. Les lignes directrices visent à clarifier les zones de recoupement entre les obligations du DMA et les principes du RGPD : - Article 5(2) DMA – Consentement : Interdiction pour les gatekeepers d'effectuer certains traitements sans le consentement valable de l'utilisateur (au sens du RGPD). Le texte précise les conditions de validité du consentement et les cas où d'autres bases légales (ex. sécurité – art. 6(1)(c) RGPD) peuvent s'appliquer. - Article 6(4) DMA – Interopérabilité des systèmes d'exploitation : Les gatekeepers doivent permettre l'installation et l'usage effectif d'applications ou magasins d'applications tiers, tout en respectant le RGPD et la directive ePrivacy. Les mesures de conformité au RGPD doivent affecter le moins possible les objectifs du DMA. - Article 6(9) DMA – Portabilité des données : Ce droit complète l'article 20 du RGPD. Les lignes directrices précisent les modalités de portabilité des données vers des tiers, la vérification de l'identité des utilisateurs et les conditions applicables aux transferts hors de l'Espace économique européen.	

			- Article 6(10) DMA – Accès aux données des utilisateurs par les entreprises : Les entreprises utilisant les plateformes doivent obtenir le consentement des utilisateurs pour accéder à leurs données. Les gatekeepers doivent faciliter la collecte et le retrait du consentement, et informer sur les responsables de traitement distincts. - Article 6(11) DMA – Partage de données de recherche : Obligation de fournir aux moteurs de recherche tiers des données d'usage anonymisées (clics, requêtes, classements). L'objectif est de renforcer la concurrence tout en assurant une anonymisation effective. - Article 7 DMA – Interopérabilité des services de communication : Les gatekeepers doivent offrir une interopérabilité avec d'autres services tout en respectant les principes de minimisation des données et de sécurité du RGPD. Les lignes directrices insistent sur la coopération étroite entre la Commission européenne (chargée de l'application du DMA) et les autorités de protection des données (garantes du RGPD).	
LE COIN RÉGLEMENTATION	15/10/2025	LINC – Cahiers Innovation & Prospective - Nos données après nous – Octobre 2025 *LINC = Laboratoire d'innovation numérique de la CNIL*	Le 10e cahier Innovation et Prospective (IP10) du LINC explore les enjeux liés aux données post mortem, de la gestion des comptes numériques à l'émergence d'agents conversationnels reproduisant le comportement des défunts. Selon une enquête Harris Interactive-CNIL (novembre 2024), près d'un tiers des Français ont déjà rencontré du contenu provenant de comptes de personnes décédées. Pourtant, la moitié des Français souhaiterait que leurs publications soient supprimées après leur décès, un souhait plus marqué chez les plus âgés. Ces chiffres illustrent	Pour information

			l'importance croissante de la gestion de l'identité numérique post mortem. Le RGPD ne considère pas les données des personnes décédées comme personnelles, laissant aux États le soin de définir des règles locales. La France prévoit certaines dispositions via la Loi Informatique et Libertés, mais les pratiques varient à l'international. Les nouvelles technologies soulèvent également des questions éthiques, comme le droit à ne pas devenir un agent conversationnel ou « deadbot ». De nombreux services en ligne proposent la gestion des comptes et des données après décès, du paramétrage ante mortem aux interactions post mortem. Des solutions plus avancées permettent désormais de créer des agents conversationnels personnalisés, ouvrant la voie à une forme d'immortalité numérique. Ce cahier du LINC encourage la gestion proactive des données, l'éducation aux risques numériques et le développement de standards pour les parcours utilisateurs post mortem. La réflexion sur la mort numérique devient ainsi essentielle, tant pour protéger la mémoire des défunts que pour anticiper les enjeux techniques et éthiques.	
 LE COIN RÉGLEMENTATION	16/10/2025	EDPS - Opinion 26-2025 on the Recommendation for a Council Decision authorising the opening of negotiations for a digital trade agreement with Canada – October 2025 *EDPS = European Data Protection Supervisor* *ou Contrôleur européen de la protection des données en français*	Le 10 septembre 2025, la Commission européenne a recommandé au Conseil de l'Union européenne (« UE ») d'autoriser l'ouverture de négociations pour un accord de commerce numérique (Digital Trade Agreement – DTA) avec le Canada, destiné à compléter l'accord de libre-échange CETA déjà en vigueur depuis 2017. Cet accord s'inscrirait dans le cadre du Partenariat numérique UE–Canada lancé en 2023. Il vise à établir des règles communes sur le commerce numérique entre les deux partenaires. L'EDPS rappelle que la protection des données personnelles est un droit fondamental dans l'Union et ne peut pas faire l'objet de négociations commerciales.	 Pour information

			Les flux transfrontaliers de données doivent rester régis par le cadre juridique européen, autrement dit le RGPD, via les mécanismes prévus (comme les décisions d'adéquation), et non par des engagements commerciaux. Il souligne que les négociations commerciales et la coopération en matière de protection des données doivent suivre des voies séparées. Le Canada bénéficie déjà d'une décision d'adéquation de la Commission européenne depuis 2002, toujours valide ; l'EDPS s'interroge donc sur la nécessité d'ajouter de nouvelles règles relatives aux flux de données dans le futur accord. Il recommande de clarifier que l'UE et ses États membres doivent pouvoir exiger, dans certains cas justifiés, la conservation des données personnelles dans l'Espace économique européen.	
LE COIN RÉGLEMENTATION	16/10/2025	CNIL - IA et vie privée : comment s'opposer à la réutilisation de ses données personnelles pour l'entraînement d'agents conversationnels ? - Octobre 2025	De nombreuses entreprises d'IA collectent les données personnelles des utilisateurs pour entraîner leurs modèles conversationnels. La CNIL détaille les démarches permettant de s'opposer à cette réutilisation pour les principales plateformes.	Pour information
LE COIN RÉGLEMENTATION	21/10/2025	EDPS - Formal comments on draft Implementing Regulation on application of Regulation (EU) No 910/2014 regarding formats of advanced electronic signatures and seals to be recognised by public sector bodies and repealing Implementing Decision (EU) 2015/1506 - October 2025	L'EDPS a été par la Commission européenne sur un projet de règlement d'exécution du règlement eIDAS (n° 910/2014), qui vise à définir les formats techniques standardisés des signatures et cachets électroniques avancés devant être reconnus par les autorités publiques de l'Union. Ce projet de règlement d'exécution remplace la décision d'exécution (UE) 2015/1506, devenue obsolète, afin de tenir compte des évolutions technologiques, des nouvelles pratiques de signature électronique et des standards internationaux.	Pour information

			L'objectif principal est de renforcer l'interopérabilité transfrontière des transactions électroniques dans l'UE et de faciliter la reconnaissance mutuelle des signatures et cachets électroniques avancés, notamment dans le contexte du cadre européen d'identité numérique. L'EDPS accueille favorablement ce projet, en soulignant plusieurs points essentiels : - Conformité au droit de la protection des données : l'EDPS salue la mention explicite de l'applicabilité du RGPD et, le cas échéant, de la directive ePrivacy, pour tout traitement de données personnelles lié à l'utilisation de signatures électroniques ; - Mise à jour continue : il se félicite de la volonté de la Commission de réviser régulièrement les spécifications techniques afin de rester en phase avec les avancées technologiques et les meilleures pratiques, conformément aux principes de protection des données dès la conception et par défaut ; - Protection renforcée de la vie privée : l'EDPS regrette que les normes techniques mentionnées ne prévoient pas encore l'utilisation de protocoles cryptographiques avancés favorisant la minimisation des données, comme les preuves à divulgation sélective ou les preuves à connaissance nulle (zero-knowledge proofs), qui permettraient d'assurer l'anonymat et la non-corrélation des transactions électroniques. - Il encourage la Commission à poursuivre ses travaux avec les organismes de normalisation (notamment l'ETSI) et les parties prenantes afin d'intégrer à l'avenir ces technologies de	

			préservation de la vie privée, essentielles pour garantir un haut niveau de confiance et de conformité au RGPD.	
LE COIN RÉGLEMENTATION	21/10/2025	EDPS - Formal comments on the draft Implementing Regulation establishing rules for the application of Regulation (EU) 2018/1727, regarding technical specifications, measures and requirements for decentralised IT system - October 2025	L'EDPS a été consulté par la Commission européenne sur un projet de règlement d'exécution du règlement (UE) 2018/1727 (relatif à Eurojust), tel que modifié par le règlement (UE) 2023/2131. Ce projet de règlement d'exécution vise à établir les spécifications techniques, mesures de sécurité et exigences opérationnelles pour la mise en place et l'utilisation d'un système informatique décentralisé destiné à permettre la communication numérique sécurisée entre Eurojust et les autorités nationales compétentes, notamment dans le domaine de la coopération judiciaire en matière pénale et de la lutte contre le terrorisme. L'EDPS a formulé quelques observations : - Il insiste sur l'importance d'un journal d'audit complet (logs) pour garantir la responsabilité et la traçabilité des accès et opérations. Il recommande d'introduire des champs de journalisation obligatoires harmonisés dans les systèmes interconnectés, notamment dans e-Codex, afin d'assurer une chaîne de contrôle ininterrompue permettant d'identifier précisément les utilisateurs et actions ; - Il encourage la Commission à compléter le texte par des informations techniques plus détaillées (architecture système, flux de données, mécanismes de sécurité, interfaces entre systèmes), pour garantir la cohérence et la sécurité globale du dispositif.	Pour information

			L'EDPS estime que le projet de règlement d'exécution constitue une base solide pour un échange d'informations sécurisé entre Eurojust et les autorités nationales.	
LE COIN RÉGLEMENTATION	21/10/2025	EDPS - Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic archiving services - October 2025	L'EDPS a été consulté par la Commission européenne sur un projet de règlement d'exécution pris en application de du règlement (UE) n° 910/2014 (eIDAS). Ce projet vise à établir les normes de référence et spécifications techniques applicables aux services d'archivage électronique qualifiés, dans le but d'assurer leur interopérabilité, leur fiabilité et leur reconnaissance mutuelle au sein du marché intérieur. Un prestataire de services de confiance conforme aux exigences de ce texte pourrait être présumé conforme aux obligations du règlement eIDAS, ce qui faciliterait l'octroi ou le maintien du statut de prestataire qualifié. L'EDPS approuve la démarche de la Commission visant à moderniser les référentiels techniques des services de confiance, tout en soulignant que la protection des données personnelles doit rester un critère central de l'élaboration, de la mise à jour et de l'évaluation de ces normes.	Pour information
LE COIN RÉGLEMENTATION	21/10/2025	EDPS - Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic ledgers - October 2025	L'EDPS a été consulté par la Commission européenne sur un projet de règlement d'exécution pris en application du règlement (UE) n° 910/2014 (eIDAS). Ce texte vise à fixer la liste des normes et spécifications de référence applicables à l'enregistrement des données électroniques dans les registres électroniques qualifiés, afin de garantir leur intégrité, leur ordre chronologique et leur fiabilité. Ces registres (ou ledgers) sont définis comme des séquences de données électroniques dont la cohérence et la traçabilité sont assurées. Lorsqu'ils sont gérés par un prestataire de services de confiance qualifié, ils peuvent bénéficier du statut de registre électronique qualifié au sens du règlement eIDAS.	Pour information

			L'EDPS note que, faute de standardisation complète, ce règlement d'exécution ne couvre actuellement que les registres électroniques distribués qualifiés, limitant donc la portée de la présomption de conformité prévue par le règlement eIDAS. Il attire particulièrement l'attention sur la question de l'immuabilité — c'est-à-dire l'impossibilité de modifier ou supprimer les enregistrements une fois inscrits dans le registre — qui est mise en avant dans le projet de règlement. Il rappelle que ni le règlement eIDAS, ni sa définition des registres électroniques n'exigent l'immuabilité, mais seulement la garantie d'intégrité et d'ordre chronologique exact. Dès lors, l'EDPS recommande de reformuler le considérant 2 du texte afin de préciser que l'immuabilité peut être une propriété utile pour certains cas d'usage, mais n'est pas obligatoire pour tous les registres qualifiés. Il insiste sur le fait que le règlement eIDAS est technologiquement neutre, et ne prescrit pas l'usage de la blockchain, ni d'une technologie particulière : seule la fonctionnalité compte. En outre, l'EDPS souligne un risque fondamental de conflit entre : - La propriété d'immuabilité qui empêche toute modification ou suppression, et - Le principe de limitation de la conservation prévu à l'article 5(1)(e) du RGPD, qui impose d'effacer ou d'anonymiser les données personnelles lorsqu'elles ne sont plus nécessaires. L'EDPS met en garde contre les difficultés de mise en conformité lorsque des données personnelles sont inscrites dans un registre immuable.	

			Si l'EDPS reconnaît que la blockchain est souvent utilisée comme technologie de registre, il rappelle qu'elle n'est pas adaptée à tous les cas d'usage et qu'elle peut exiger des garanties supplémentaires. L'EDPS renvoie à la Guideline 02/2025 du Comité européen de la protection des données (CEPD/EDPB) sur le traitement des données personnelles dans les technologies blockchain, qui propose des critères pour assurer la licéité et la minimisation des données. L'EDPS invite la Commission à vérifier que les spécifications techniques du projet tiennent compte de ces recommandations.	
LE COIN RÉGLEMENTATION	21/10/2025	EDPS - Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards for qualified certificates for website authentication - October 2025	L'EDPS a été consulté par la Commission européenne sur un projet de règlement d'exécution pris en application du règlement (UE) n° 910/2014 (eIDAS). Le projet de règlement d'exécution vise à définir les normes de référence pour la délivrance de certificats qualifiés pour l'authentification de sites web (Qualified Website Authentication Certificates – « QWACs »). Ces certificats ont pour finalité d'authentifier l'identité d'un site web et de renforcer la confiance et la transparence dans les interactions en ligne, en permettant aux utilisateurs de vérifier qu'ils se connectent à un site légitime. Les standards proposés permettraient la délivrance de QWACs sous plusieurs formes (certificats autonomes, liés à d'autres certificats, ou dans d'autres configurations techniques), afin de garantir interopérabilité, flexibilité et sécurité dans l'ensemble de l'Union européenne. Le texte veille à ne pas restreindre la liberté des fournisseurs de navigateurs web dans la gestion de la sécurité, de l'authentification des domaines et du chiffrement du trafic. L'EDPS note positivement que l'une des normes de référence prévues dans le projet aborde directement des aspects de protection des données, notamment :	Pour information

			- La confidentialité des données d'enregistrement et des journaux de certification ; - La protection de l'accès aux données personnelles traitées dans le cadre de la délivrance des certificats ; - La gestion du consentement des utilisateurs. Ces garanties visent à éviter la divulgation ou l'utilisation abusive des données des titulaires de certificats ou des administrateurs de sites web. L'EDPS encourage la surveillance continue de l'évolution des technologies d'authentification et des pratiques des prestataires de services de confiance, pour s'assurer que les futures mises à jour des standards restent conformes au droit de la protection des données.	
LE COIN RÉGLEMENTATION	21/10/2025	EDPS - Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards requirements for qualified trust service providers providing qualified trust services - October 2025	L'EDPS a été consulté par la Commission européenne sur un projet de règlement d'exécution fixant les règles d'application de l'article 24(5) du règlement (UE) n° 910/2014 (eIDAS), qui encadre les prestataires de services de confiance qualifiés. L'objectif du projet de règlement d'exécution est de définir les exigences, normes de référence et spécifications applicables aux prestataires de services de confiance fournissant des services qualifiés (ex. : signature électronique, cachet électronique, horodatage, services d'archivage, etc.). Ces normes permettent aux autorités de présumer la conformité d'un prestataire aux exigences du règlement eIDAS s'il les respecte, facilitant ainsi la qualification ou la reconnaissance du statut qualifié. L'EDPS émet un avis globalement favorable au projet de règlement d'exécution, estimant qu'il : - Renforce la sécurité, la confiance et la transparence des services de confiance qualifiés ;	Pour information

			- Intègre de manière adéquate les principes du RGPD, notamment la protection dès la conception et par défaut ; - Encourage une supervision harmonisée des prestataires dans toute l'UE. Cependant, il recommande explicitement d'inclure une obligation de documentation du consentement, afin de garantir une conformité complète avec le droit à la protection des données personnelles. En effet, l'article 24(2)(f)(i) du règlement eIDAS impose que les prestataires conservent certaines données « sous une forme vérifiable » et ne les rendent publiquement accessibles que si la personne concernée y a consenti. L'EDPS recommande donc d'ajouter dans le projet une obligation explicite pour les prestataires de : - Documenter la procédure de gestion du consentement ; - Démontrer comment ce consentement est recueilli, conservé et respecté dans le temps.	
LE COIN RÉGLEMENTATION	24/10/2025	EDPB - Opinion 23-2025 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the Tessi Group - October 2025	L'EDPB s'est prononcé sur un projet de décision de règles d'entreprises contraignantes (« BCR ») de responsable de traitement pour le groupe Tessi, soumise par l'autorité de protection des données française, en tant qu'autorité chef de file. Le groupe Tessi est un groupe français spécialisé dans la transformation digitale et les services transactionnels. L'EDPB a conclu que le projet de BCR soumis contenait tous les éléments requis en vertu du RGPD.	Pour information

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	24/10/2025	EDPB - Opinion 24-2025 on the decision of the Polish Supervisory Authority regarding the Controller Binding Corporate Rules of the BOX Group - October 2025	L'EDPB s'est prononcé sur un projet de décision de règles d'entreprises contraignantes (« BCR ») de responsable de traitement pour le groupe BOX, soumise par l'autorité de protection des données polonaise, en tant qu'autorité chef de file. Le groupe BOX est un groupe international agissant notamment dans la gestion et traitement des données et services cloud et des solutions digitales pour entreprises. Le groupe BOX avait déjà soumis des BCR-responsable de traitement sous la directive 95/46/CE, approuvées par l'autorité britannique. Après le Brexit, des modifications étaient nécessaires pour identifier une autorité chef de file au sein de l'Espace économique européenne et adapter le texte au RGPD. L'autorité polonaise a accepté d'agir comme autorité chef de file pour le groupe. L'EDPB a conclu que le projet de BCR soumis contenait tous les éléments requis en vertu du RGPD.	Pour information
LE COIN RÉGLEMENTATION	24/10/2025	EDPB - Opinion 25-2025 on the decision of the Polish Supervisory Authority regarding the Processor Binding Corporate Rules of the BOX Group - October 2025	L'EDPB s'est prononcé sur un projet de décision de règles d'entreprises contraignantes (« BCR ») de sous-traitant pour le groupe BOX, soumise par l'autorité de protection des données polonaise, en tant qu'autorité chef de file. Le groupe BOX avait déjà soumis des BCR-sous-traitant sous la directive 95/46/CE, approuvées par l'autorité britannique. Après le Brexit, des modifications étaient nécessaires pour identifier une autorité chef de file au sein de l'Espace économique européenne et adapter le texte au RGPD. L'autorité polonaise a accepté d'agir comme autorité chef de file pour le groupe. L'EDPB a conclu que le projet de BCR soumis contenait tous les éléments requis en vertu du RGPD.	Pour information

Icônes « Quelles actions ? » by Adrien Coquet

LE COIN RÉGLEMENTATION	24/10/2025	EDPB - Opinion 26-2025 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by the United Kingdom - October 2025	La Commission européenne a lancé en juillet 2025 le renouvellement de la décision d'adéquation concernant le Royaume-Uni, qui permet le transfert sécurisé des données personnelles. Saisi pour avis, l'EDPB reconnaît que le cadre britannique reste globalement conforme au RGPD, mais alerte sur plusieurs évolutions législatives récentes susceptibles d'affaiblir la protection des données, notamment la fin de la primauté du droit européen et l'élargissement des pouvoirs gouvernementaux. - Un suivi étroit est demandé avant confirmation finale de l'adéquation, valable jusqu'en 2031.	Pour information
LE COIN RÉGLEMENTATION	24/10/2025	EDPB – Opinion 27-2025 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data by the United Kingdom – October 2025	La Commission européenne a présenté son projet de décision d'adéquation reconnaissant que le Royaume-Uni assure un niveau de protection adéquat pour les données à caractère personnel traitées dans le cadre de l'application de la loi en vertu de la Directive (UE) 2016/680, c'est-à-dire le cadre des transferts de données à des fins de police et de justice pénale. L'EDPB ne s'oppose pas à la reconduction de la décision d'adéquation, mais soulève des réserves substantielles sur certaines évolutions récentes du droit britannique, notamment : - Les transferts internationaux, le Royaume-Uni ayant modifié les critères d'évaluation de l'équation pour les transferts de données vers d'autres pays et ayant introduit un critère de « désirabilité de faciliter les transferts » jugé trop flou par l'EDPB ; - La prise de décision automatisée, le secrétaire d'Etat ayant des pouvoirs plus étendus ; - Et les exemptions de sécurité nationale plus larges qu'auparavant.	

			L'EDPB invite la Commission européenne à compléter son évaluation finale et à assurer un suivi étroit et continu des pratiques britanniques dans le domaine du traitement des données à des fins répressives.	
LE COIN RÉGLEMENTATION	31/10/2025	European Parliament - Interplay between the AI Act and the EU digital legislative framework - October 2025	La Commission ITRE du Parlement européen (commission de l'industrie, de la recherche et de l'énergie – Committee on industry, research and energy) a rendu un rapport sur le règlement Intelligence Artificielle (« IA Act ») et son articulation avec les autres textes européens régissant l'économique numérique : RGPD, Data Act, DSA, DMA, Cyber Resilience Act, NIS2, etc. Ce rapport analyse les interactions entre ces différentes lois et cherche à déterminer : - Si elles forment un système cohérent, - Ou si, au contraire, elles produisent des chevauchements, incohérences et charges excessives qui risquent de freiner l'innovation et la compétitivité européenne. Le rapport identifie de nombreuses zones de friction entre le AI Act et les autres instruments du "puzzle" numérique européen : - Avec le RGPD : les évaluations d'impact sur les droits fondamentaux et les évaluations d'impact sur la protection des données se recoupent sans s'aligner ; - Avec le Data Act : double régime pour les fournisseurs d'IA qui sont aussi détenteurs de données : accès, portabilité et partage imposent une charge cumulative de conformité, notamment pour les tests et transferts internationaux ; - Avec le Cyber Résilience Act (« CRA ») : les exigences de cybersécurité du CRA et du AI Act ne s'alignent que partiellement. Certaines	

			certifications peuvent être mutuellement reconnues, mais il subsiste des zones d'ambiguïté ; - Avec le Digital Services Act (« DSA ») : les grandes plateformes utilisant des IA (modération, recommandation, recherche) sont soumises à des obligations de transparence et d'évaluation des risques similaires. Cela crée une double régulation, notamment pour les IA génératives intégrées aux services ; - Avec le Digital Market Act (« DMA ») : les "gatekeepers" proposant des API ou modèles d'IA peuvent être affectés par les règles d'interopérabilité et d'accès aux données, même si les systèmes d'IA ne sont pas encore formellement désignés comme "core platform services" ; - Avec la directive NIS2 : les obligations en matière de gestion du risque et notification d'incidents se recoupent avec celles du AI Act, notamment pour les entités essentielles développant ou utilisant de l'IA. En outre, l'AI Act crée un nouvel organe, le European AI Office (AIO), chargé de : - Superviser les modèles d'IA à usage général, - Coordonner les autorités nationales, - Gérer les bacs à sable réglementaires. Mais : - Ses compétences se chevauchent avec celles des autorités de protection des données, des organismes de surveillance du marché ou du Comité européen de la protection des données ;	

			- Son ancrage au sein de la Commission sans personnalité juridique propre soulève des questions d'indépendance et de capacité opérationnelle. Le rapport alerte sur le risque de sur-réglementation cumulative dans l'Union : - Les obligations sont justifiées isolément, mais leur superposition freine l'innovation, retarde la mise sur le marché et désavantage les PME européennes ; - Les grandes entreprises, souvent non européennes, disposent des ressources pour absorber ces coûts de conformité ; - L'Union européenne pourrait ainsi ralentir sa capacité à créer des champions mondiaux de l'IA, malgré son ambition de promouvoir une IA « fiable et centrée sur l'humain ». La Commission ITRE a formulé différentes recommandations : - A court terme : o Élaborer des orientations communes entre autorités (ex. EDPB, AI Office, autorités de marché) ; o Mettre en place la reconnaissance mutuelle entre analyses d'impact de protection des données et de protection des droits fondamentaux ; o Harmoniser les procédures de bacs à sable entre États membres. - A moyen terme : o Introduire des ajustements législatifs légers pour :	

			▪ Clarifier les rôles entre acteurs (fournisseurs, déployeurs, autorités), ▪ Réduire les obligations redondantes (surtout en matière de droits fondamentaux et cybersécurité), ▪ Améliorer la mise en œuvre pratique des droits des personnes dans les contextes IA. - A long terme o Repenser l'architecture numérique européenne pour plus de cohérence. Le rapport reconnaît que l'AI Act est une avancée majeure pour un développement éthique et sûr de l'intelligence artificielle. Mais il avertit qu'en l'état, il s'intègre dans un écosystème réglementaire trop fragmenté et lourd. Sans meilleure cohérence, coordination institutionnelle et souplesse pour les innovateurs, l'Union européenne risque de transformer son ambition de leadership en un handicap compétitif.	
LE COIN RÉGLEMENTATION	31/10/2025	Haute Autorité de santé - Premières clefs d'usage de l'IA générative en santé - 30 octobre 2025	La Haute Autorité de santé (« HAS ») publie un guide pour promouvoir un usage responsable de l'IA générative (ChatGPT, Mistral AI, Copilot, etc.) dans les secteurs sanitaire, social et médico-social. Ces outils, capables de produire du texte, des images ou des synthèses, offrent un potentiel d'efficacité et d'amélioration des pratiques. Mais ils présentent aussi des risques : erreurs factuelles, atteintes à la confidentialité et manque de transparence. Le guide s'articule autour de quatre principes clés – A.V.E.C. : - Apprendre à comprendre et maîtriser l'outil, - Vérifier la fiabilité et la confidentialité des contenus, - Estimer la pertinence des usages au fil du temps,	Pour information

Icônes « Quelles actions ? » by Adrien Coquet

			- Communiquer avec les pairs et les patients pour garantir la transparence. Cette publication constitue la première étape du cadre de confiance de la HAS sur l'usage de l'IA en santé, avant d'autres travaux à venir pour les usagers et établissements.	